DISCUSSION DRAFT OF H.R. _____, A BILL TO REQUIRE GREATER PROTECTION FOR SENSITIVE CONSUMER DATA AND TIMELY NOTIFICATION IN CASE OF BREACH

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JUNE 15, 2011

Serial No. 112–62

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

71–568 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MARY BONO MACK, California
Chairman

MARSHA BLACKBURN, Tennessee
Vice Chair
CLIFF STEARNS, Florida
CHARLES F. BASS, New Hampshire
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVE B. McKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
JOE BARTON, Texas
FRED UPTON, Michigan, *ex officio*

G.K. BUTTERFIELD, North Carolina
Ranking Member
CHARLES A. GONZALEZ, Texas
JIM MATHESON, Utah
JOHN D. DINGELL, Michigan
EDOLPHUS TOWNS, New York
BOBBY L. RUSH, Illinois
JANICE D. SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
HENRY A. WAXMAN, California, *ex officio*

CONTENTS

DISCUSSION DRAFT OF H.R. ———, A BILL TO REQUIRE GREATER PROTECTION FOR SENSITIVE CONSUMER DATA AND TIMELY NOTIFICATION IN CASE OF BREACH

WEDNESDAY, JUNE 15, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:30 a.m., in room 2322, Rayburn House Office Building, Hon. Mary Bono Mack (chairwoman of the subcommittee) presiding.

Present: Representatives Bono Mack, Blackburn, Stearns, Bass, Harper, Lance, Cassidy, Guthrie, Olson, Pompeo, Kinzinger, Butterfield, Gonzalez, Dingell, Towns, Rush, Schakowsky, and Waxman (ex officio).

Staff Present: Allison Busbee, Legislative Clerk; Paul Cancienne, Policy Coordinator, CMT; Brian McCullough, Sr. Professional Staff Member, CMT; Gib Mullan, Chief Counsel, CMT; Shannon Weinberg, Counsel, CMT; Michelle Ash, Democratic Chief Counsel; Felipe Mendoza, Democratic Counsel; and Will Wallace, Democratic Policy Analyst.

Mrs. BONO MACK. Good morning. The subcommittee will now come to order. Today hackers and online thieves are giving more meaning to the phrase silent crime. It is my hope that we will join together, raise our voices and, like after Peter Finch in the movie "Network," shout out the window, we are mad as hell, and we are not going to take this anymore. Americans deserve nothing less.

[The discussion draft follows:]

[DISCUSSION DRAFT]

JUNE 10, 2011

112TH CONGRESS
1ST SESSION

H. R. _____

To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach.

IN THE HOUSE OF REPRESENTATIVES

Mrs. BONO MACK introduced the following bill; which was referred to the Committee on _____

A BILL

To protect consumers by requiring reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a security breach.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure and Fortify Electronic Data Act" or the "SAFE Data Act".

SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

(a) GENERAL SECURITY POLICIES AND PROCEDURES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require any person engaged in interstate commerce that owns or possesses data containing personal information related to that commercial activity, including an information broker and any third party that has contracted with such person to maintain such data on behalf of such person, to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information, taking into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by, such person;

(B) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(C) the cost of implementing such safeguards.

(2) DATA SECURITY REQUIREMENTS.—Such regulations shall require the policies and procedures to include the following:

(A) A security policy with respect to the collection, use, sale, other dissemination, and maintenance of such personal information.

(B) The identification of an officer [or other individual] as the point of contact with responsibility for the management of information security.

(C) A process for identifying and assessing any reasonably foreseeable vulnerabilities in each system maintained by such person that contains such data, which shall include regular monitoring for a breach of security of each such system.

(D) A process for taking preventive and corrective action to mitigate against any vulnerabilities identified in the process required by subparagraph (C), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software.

(E) A process for disposing of data in electronic form containing personal information by

shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable.

(F) A standard method or methods for the destruction of paper documents and other non-electronic data containing personal information.

[(3) DATA MINIMIZATION REQUIREMENTS.—A person subject to the requirements under paragraph (1) shall establish a plan and procedures for minimizing the amount of data containing personal information maintained by such person. Such a plan and procedures shall provide for the retention of such personal information only as reasonably needed for the legitimate business purposes of such person or as necessary to comply with any legal obligation.]

(b) TREATMENT OF ENTITIES GOVERNED BY HIPAA AND GRAMM-LEACH-BLILEY.—Any person who is subject to the requirements of part C of title XI of the Social Security Act 42 U.S.C. 1301 et seq.) or title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) to maintain standards and safeguards for information security and protection of personal information shall be exempt from the requirements of this Act for any activities governed by such requirements under such Acts.

(c) EXEMPTION FOR CERTAIN SERVICE PROVIDERS.—Nothing in this section shall apply to a service provider for any electronic communication by a third party that is transmitted, routed, or stored in intermediate or transient storage by such service provider.

SEC. 3. NOTIFICATION AND OTHER REQUIREMENTS IN THE EVENT OF A BREACH OF SECURITY.

(a) REQUIREMENTS IN THE EVENT OF A BREACH OF SECURITY.—Any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information related to that commercial activity, following the discovery of a breach of security of any system maintained by such person that contains such data, shall—

(1)(A) notify appropriate law enforcement officials of the breach of security not later than 48 hours after such discovery, unless the breach of security involved only inadvertent access to or inadvertent acquisition of data by an employee or agent of such person; and

(B) if the person subsequently determines that the breach of security was not inadvertent, notify appropriate law enforcement officials of the breach of security not later than 48 hours after such determination;

(2) assess the nature and scope of such a breach of security, take such steps necessary to prevent further breach or unauthorized disclosures, and reasonably restore the integrity of the data system; and

(3) not later than 48 hours after completing the assessment required under paragraph (2), if the person determines, based on such assessment, that the breach of security presents a reasonable risk of identity theft, fraud, or other unlawful conduct—

(A) notify the Commission; and

(B) begin to notify as promptly as possible, subject to subsection (c), each individual who is a citizen or resident of the United States whose personal information was acquired or accessed as a result of such a breach of security.

(b) SPECIAL NOTIFICATION REQUIREMENTS.—

(1) THIRD PARTY AGENTS.—In the event of a breach of security of any third party entity that has contracted with a person to maintain or process data in electronic form containing personal information on behalf of such person, such third party entity shall be required to notify such person of the breach of security. Upon receiving such notification from

the third party, such person shall take the actions required under subsection (a).

(2) SERVICE PROVIDERS.—If a service provider becomes aware of a breach of security of data in electronic form containing personal information that is owned or possessed by another person that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, such service provider shall be required to notify of such a breach of security only the person who initiated such connection, transmission, routing, or storage if such person can be reasonably identified. Upon receiving such notification from a service provider, such person shall take the action required under subsection (a).

(3) COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.—If a person is required to provide notification to more than 5,000 individuals under subsection (a)(3)(B), the person shall also notify the major credit reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing and distribution of the notices. Such notice shall be given to the credit reporting agencies without unreasonable delay and,

if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(c) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(1) LAW ENFORCEMENT.—If a Federal, State, or local law enforcement agency determines that the notification required under subsection (a)(3)(B) would impede a civil or criminal investigation, such notification shall be delayed upon the request of the law enforcement agency for 30 days or such lesser period of time which the law enforcement agency determines is reasonably necessary. The law enforcement agency shall follow up such a request in writing. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period of time set forth in the original request made under this paragraph if further delay is necessary.

(2) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under subsection (a)(3)(B) would threaten national or homeland security, such notification may be delayed for a period of time which the national security agency or homeland security agency determines is reason-

ably necessary. The national security agency or homeland security agency shall follow up such a request in writing. A Federal national security agency or homeland security agency may revoke such delay or extend the period of time set forth in the original request made under this paragraph by a subsequent written request if further delay is necessary.

(d) METHOD AND CONTENT OF NOTIFICATION.—

(1) DIRECT NOTIFICATION.—

(A) METHOD OF NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(1)(B) shall be in compliance with such requirement if the person provides conspicuous and clearly identified notification by one of the following methods (provided the selected method can reasonably be expected to reach the intended individual):

(i) Written notification.

(ii) Notification by email or other electronic means, if—

(I) the person's primary method of communication with the individual is by email or such other electronic means; or

(II) the individual has consented to receive such notification and the notification is provided in a manner that is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global Commerce Act (15 U.S.C. 7001).

(B) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subparagraph (A), such notification shall include—

(i) a description of the personal information that was acquired or accessed by an unauthorized person;

(ii) a telephone number that the individual may use, at no cost to such individual, to contact the person to inquire about the breach of security or the information the person maintained about that individual;

(iii) notice that the individual is entitled to receive, at no cost to such individual, consumer credit reports on a quarterly basis for a period of 2 years, or credit

monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 2 years, and instructions to the individual on requesting such reports or service from the person, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code;

(iv) the toll-free contact telephone numbers and addresses for the major credit reporting agencies; and

(v) a toll-free telephone number and Internet website address for the Commission whereby the individual may obtain information regarding identity theft.

(2) SUBSTITUTE NOTIFICATION.—

(A) CIRCUMSTANCES GIVING RISE TO SUBSTITUTE NOTIFICATION.—A person required to provide notification to individuals under subsection (a)(1) may provide substitute notification in lieu of the direct notification required by

paragraph (1) if the person owns or possesses data in electronic form containing personal information of fewer than 1,000 individuals and such direct notification is not feasible due to—

(i) excessive cost to the person required to provide such notification relative to the resources of such person, as determined in accordance with the regulations issued by the Commission under paragraph (3)(A); or

(ii) lack of sufficient contact information for the individual required to be notified.

(B) FORM OF SUBSTITUTE NOTIFICATION.—Such substitute notification shall include—

(i) email notification to the extent that the person has email addresses of individuals to whom it is required to provide notification under subsection (a)(1);

(ii) a conspicuous notice on the Internet website of the person (if such person maintains such a website); and

(iii) notification in print and to broadcast media, including major media in met-

ropolitan and rural areas where the individuals whose personal information was acquired reside.

(C) CONTENT OF SUBSTITUTE NOTICE.—Each form of substitute notice under this paragraph shall include—

(i) notice that individuals whose personal information is included in the breach of security are entitled to receive, at no cost to the individuals, consumer credit reports on a quarterly basis for a period of 2 years, or credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 2 years, and instructions on requesting such reports or service from the person, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code; and

(ii) a telephone number by which an individual can, at no cost to such indi-

vidual, learn whether that individual's personal information is included in the breach of security.

(3) REGULATIONS AND GUIDANCE.—

(A) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by regulation under section 553 of title 5, United States Code, establish criteria for determining circumstances under which substitute notification may be provided under paragraph (2), including criteria for determining if notification under paragraph (1) is not feasible due to excessive costs to the person required to provide such notification relative to the resources of such person. Such regulations may also identify other circumstances where substitute notification would be appropriate for any person, including circumstances under which the cost of providing notification exceeds the benefits to consumers.

(B) GUIDANCE.—In addition, the Commission shall provide and publish general guidance with respect to compliance with this subsection. Such guidance shall include—

(i) a description of written or email notification that complies with the requirements of paragraph (1); and

(ii) guidance on the content of substitute notification under paragraph (2), including the extent of notification to print and broadcast media that complies with the requirements of such paragraph.

(e) OTHER OBLIGATIONS FOLLOWING BREACH.—

(1) IN GENERAL.—A person required to provide notification under subsection (a) shall, upon request of an individual whose personal information was included in the breach of security, provide or arrange for the provision of, to each such individual and at no cost to such individual—

(A) consumer credit reports from at least one of the major credit reporting agencies beginning not later than 60 days following the individual's request and continuing on a quarterly basis for a period of 2 years thereafter; or

(B) a credit monitoring or other service that enables consumers to detect the misuse of their personal information, beginning not later than 60 days following the individual's request and continuing for a period of 2 years.

(2) LIMITATION.—This subsection shall not apply if the only personal information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—As part of the Commission's rulemaking described in subsection (d)(3), the Commission shall determine the circumstances under which a person required to provide notification under subsection (a)(1) shall provide or arrange for the provision of free consumer credit reports or credit monitoring or other service to affected individuals.

(f) EXEMPTION BASED ON ASSESSMENT OF RISK AND PRESUMPTION.—

(1) GENERAL EXEMPTION.—A person shall be exempt from the requirements under this section if, following a breach of security, such person determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

(2) PRESUMPTION.—

(A) IN GENERAL.—If the data in electronic form containing personal information is rendered unusable, unreadable, or indecipherable through encryption or other security technology

or methodology (if the method of encryption or such other technology or methodology is generally accepted by experts in the information security field), there shall be a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that the encryption or other security technologies or methodologies in a specific case have been or are reasonably likely to be compromised.

(B) METHODOLOGIES OR TECHNOLOGIES.—Not later than 1 year after the date of the enactment of this Act and biannually thereafter, the Commission shall issue rules (pursuant to section 553 of title 5, United States Code) or guidance to identify security methodologies or technologies which render data in electronic form unusable, unreadable, or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that any such meth-

odology or technology in a specific case has been or is reasonably likely to be compromised. In issuing such rules or guidance, the Commission shall consult with relevant industries, consumer organizations, and data security and identity theft prevention experts and established standards setting bodies.

(3) FTC GUIDANCE.—Not later than 1 year after the date of the enactment of this Act the Commission shall issue guidance regarding the application of the exemption in paragraph (1).

(g) WEBSITE NOTICE OF FEDERAL TRADE COMMISSION.—If the Commission, upon receiving notification of any breach of security that is reported to the Commission under subsection (a)(2), finds that notification of such a breach of security via the Commission's Internet website would be in the public interest or for the protection of consumers, the Commission shall place such a notice in a clear and conspicuous location on its Internet website.

(h) FTC STUDY ON NOTIFICATION IN LANGUAGES IN ADDITION TO ENGLISH.—Not later than 1 year after the date of enactment of this Act, the Commission shall conduct a study on the practicality and cost effectiveness of requiring the notification required by subsection (d)(1)

to be provided in a language in addition to English to individuals known to speak only such other language.

(i) GENERAL RULEMAKING AUTHORITY.—The Commission may promulgate regulations necessary under section 553 of title 5, United States Code, to effectively enforce the requirements of this section.

(j) TREATMENT OF PERSONS GOVERNED BY OTHER LAW.—A person who is in compliance with any other Federal law that requires such person to provide notification to individuals following a breach of security, and that, taken as a whole, provides protections substantially similar to, or greater than, those required under this section, as the Commission shall determine by rule (under section 553 of title 5, United States Code), shall be deemed to be in compliance with this section.

SEC. 4. APPLICATION AND ENFORCEMENT.

(a) GENERAL APPLICATION.—The requirements of sections 2 and 3 apply to any information broker or other person engaged in interstate commerce that owns or posses data containing personal information related to that commercial activity, or contracts to have any third party entity maintain such data for such person, including—

(1) those persons, partnerships, or corporations over which the Commission has authority pursuant

to section 5(a)(2) of the Federal Trade Commission Act; and

(2) notwithstanding section 4 and section 5(a)(2) of that Act (15 U.S.C. 44 and 45(a)(2)), any non-profit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of such Code.

(b) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 2 or 3 shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates such regulations shall be subject to the penalties and

entitled to the privileges and immunities provided in that Act.

(3) LIMITATION.—In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.

(c) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates section 2 or 3 of this Act, the attorney general, official, or agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction—

(A) to enjoin further violation of such section by the defendant;

(B) to compel compliance with such section; or

(C) to obtain civil penalties in the amount determined under paragraph (2).

(2) CIVIL PENALTIES.—

(A) CALCULATION.—

(i) TREATMENT OF VIOLATIONS OF SECTION 2.—For purposes of paragraph (1)(C) with regard to a violation of section 2, the amount determined under this paragraph is the amount calculated by multiplying the number of days that a person is not in compliance with such section by an amount not greater than $11,000.

(ii) TREATMENT OF VIOLATIONS OF SECTION 3.—For purposes of paragraph (1)(C) with regard to a violation of section 3, the amount determined under this paragraph is the amount calculated by multiplying the number of violations of such section by an amount not greater than $11,000. Each failure to send notification as required under section 3 to a resident of the State shall be treated as a separate violation.

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of

enactment of this Act, and each year thereafter, the amounts specified in clauses (i) and (ii) of subparagraph (A) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(C) MAXIMUM TOTAL LIABILITY.—Notwithstanding the number of actions which may be brought against a person under this subsection, the maximum civil penalty for which any person may be liable under this subsection shall not exceed—

(i) $5,000,000 for each violation of section 2; and

(ii) $5,000,000 for all violations of section 3 resulting from a single breach of security.

(3) INTERVENTION BY THE FTC.—

(A) NOTICE AND INTERVENTION.—The State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon

instituting such action. The Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission has instituted a civil action for violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this Act alleged in the complaint.

(4) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

SEC. 5. DEFINITIONS.

In this Act the following definitions apply:

(1) BREACH OF SECURITY.—The term "breach of security" means any unauthorized access to or acquisition of data in electronic form containing personal information.

(2) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(3) DATA IN ELECTRONIC FORM.—The term "data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(4) ENCRYPTION.—The term "encryption" means the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data. Such encryption must include appropriate management

and safeguards of such keys to protect the integrity of the encryption.

(5) IDENTITY THEFT.—The term "identity theft" means the unauthorized use of another person's personal information for the purpose of engaging in commercial transactions under the name of such other person.

(6) INFORMATION BROKER.—The term "information broker"—

(A) means a commercial entity whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity in order to sell such information or provide access to such information to any nonaffiliated third party in exchange for consideration, whether such collection, assembly, or maintenance of personal information is performed by the information broker directly, or by contract or subcontract with any other entity; and

(B) does not include a commercial entity to the extent that such entity processes information collected by or on behalf of and received from or on behalf of a nonaffiliated third party concerning individuals who are current or

former customers or employees of such third party to enable such third party directly or through parties acting on its behalf to: (1) provide benefits for its employees; or (2) directly transact business with its customers.

(7) PERSONAL INFORMATION.—

(A) DEFINITION.—The term "personal information" means an individual's first name or initial and last name, or address, or phone number, in combination with any 1 or more of the following data elements for that individual:

(i) Social Security number.

(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

[(B) PUBLIC RECORD INFORMATION.—Such term does not include public record information.]

(C) MODIFIED DEFINITION BY RULEMAKING.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, modify the definition of "personal information" under subparagraph (A)—

(i) for the purpose of section 2 to the extent that such modification is necessary to accomplish the purposes of such section as a result of changes in technology or practices and will not unreasonably impede Internet or other technological innovation or otherwise adversely affect interstate commerce; or

(ii) for the purpose of section 3, if the Commission determines that access to or acquisition of the additional data elements in the event of a breach of security would create an unreasonable risk of identity theft, fraud, or other unlawful activity and that such modification will not unreasonably impede Internet or other technological innovation or otherwise adversely affect interstate commerce.

(8) PUBLIC RECORD INFORMATION.—The term "public record information" means information

about an individual is lawfully made available to the general public from Federal, State, or local government records

(9) SERVICE PROVIDER.—The term "service provider" means a person that provides electronic data transmission, routing, intermediate and transient storage, or connections to its system or network, where the person providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and such person transmits, routes, stores, or provides connections for personal information in a manner such that personal information is undifferentiated from other types of data that such person transmits, routes, or stores, or for which such person provides such connections. Any such person shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage or connections.

SEC. 6. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE INFORMATION SECURITY LAWS.—This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of

a State, with respect to those entities covered by the regulations issued pursuant to this Act, that expressly—

(1) requires information security practices and treatment of data containing personal information similar to any of those required under section 2; and

(2) requires notification to individuals of a breach of security resulting in unauthorized access to or acquisition of data in electronic form containing personal information.

(b) ADDITIONAL PREEMPTION.—

(1) IN GENERAL.—No person other than a person specified in section 4(c) may bring a civil action under the laws of any State if such action is premised in whole or in part upon the defendant violating any provision of this Act.

(2) PROTECTION OF CONSUMER PROTECTION LAWS.—This subsection shall not be construed to limit the enforcement of any State consumer protection law by an Attorney General of a State.

(c) PROTECTION OF CERTAIN STATE LAWS.—This Act shall not be construed to preempt the applicability of—

(1) State trespass, contract, or tort law; or

(2) other State laws to the extent that those laws relate to acts of fraud.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit or affect the Commission's authority under any other provision of law.

SEC. 7. EFFECTIVE DATE.

This Act shall take effect 1 year after the date of enactment of this Act.

OPENING STATEMENT OF HON. MARY BONO MACK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mrs. BONO MACK. The chair now recognizes herself for an opening statement. Sophisticated cyber attacks are increasingly becoming the greatest threat to the future of electronic commerce here in the U.S. and around the world. That is why Congress must take immediate steps to better protect the personal online information of American consumers. It is time for us to declare war on identity theft and online fraud.

The Secure and Fortify Electronic Data Act, which established uniform national standards for data security and data breach notification, is our opening shot. The SAFE Data Act builds on legislation passed by the House in 2009 but never acted upon in the Senate. Most importantly, it reflects the changing landscape of data breaches and data security since that time.

It is an upgraded 2.0 version of data security legislation, encompassing many of the lessons learned in the aftermath of massive data breaches at Sony and Epsilon, which put more than 100 million consumer accounts at risk, and those are just the ones that we know about.

As subcommittee chairman, protection from identity theft and online fraud is one of my top priorities. Just last week Citigroup, which has the world's largest financial services network, revealed a security breach in which hackers obtained personal information from hundreds of thousands of accounts. According to law enforcement officials, the hackers were able to gain access to customer names, account numbers and contact information, such as e-mail addresses.

Yesterday we learned that an external Web site operated by the Oak Ridge Nuclear Weapons Plant was victimized by a cyber attack, and earlier this week, the same group which claimed responsibility for attacks on Foxx, PBS and Sony also hacked the Senate's public Web site.

In recent years carefully orchestrated cyber attacks intended to obtain personal information about consumers, especially when it comes to their credit cards, have become one of the fastest growing criminal enterprises here in the United States and across the world. The FTC estimates that nearly 9 million Americans fall victim to identity theft every year, costing consumers and businesses billions of dollars annually.

And the problem is only getting worse as these online attacks increase in frequency, sophistication and boldness. As I have emphasized throughout our previous hearings e-commerce is a vital and growing part of our economy. We should take steps to embrace and protect it, and that starts with robust cybersecurity.

Most importantly, consumers have a right to know when their personal information has been compromised, and companies and organizations have an overriding responsibility to promptly alert them.

To that end, the SAFE Data Act first requires companies and other entities that hold personal information to establish and maintain appropriate security policies to prevent unauthorized acquisition of the data.

It also requires notification of law enforcement within 48 hours after discovery of a breach, unless it was an accident or inadvertent and unlikely to result in harm.

It requires companies and other entities to begin notifying consumers 48 hours after taking steps to prevent further breaches and determining who has to be notified.

The SAFE Data Act also gives the FTC authority over nonprofits for purposes of this act only. These organizations often possess a tremendous amount of consumer information, and they have been subjected to numerous breaches in the past.

At the same time, we want to work with those affected, as well as with the FTC, to make sure any new regulations are not burdensome for small businesses, especially during these difficult economic times.

In addition, we are granting the FTC authority to write rules that take into account the size and the nature of the data that is being held online. Clearly, there are obvious differences between information brokers and local retail businesses, and the rules should reflect those differences.

The proposed legislation also requires all covered businesses to establish a data minimization plan providing for the elimination of consumers' personal data that is no longer necessary for business purposes or for other legal obligations.

And finally, the SAFE Data Act preempts similar State laws to create uniform national standards for data security and data breach notification. We learned during our recent hearings that consumer notification is often hampered by the fact that companies must first determine their obligations under 47 different State regimes.

At the end of the day I, believe this legislation will greatly benefit consumers, businesses and the U.S. economy. Given the growing importance of e-commerce in nearly everything, we do we can no longer afford to sit back and do nothing. The time for action is now.

And at this point, the gentleman from—OK. And inform people that we do have an overflow room in 2123 for those standing who prefer to be sitting; again 2123 is the overflow room.

So, at this point, I would like to recognize the gentleman from California, Mr. Waxman, for his opening statement.

[The prepared statement of Mrs. Bono Mack follows:]

PREPARED STATEMENT OF HON. MARY BONO MACK

Sophisticated cyber attacks are increasingly becoming the greatest threat to the future of electronic commerce here in the United States and around the world, and that's why Congress must take immediate steps to better protect the personal online information of American consumers. It's time for us to declare war on identity theft and online fraud.

The Secure and Fortify Data Act—which establishes uniform national standards for data security and data breach notification—is our opening shot.

The SAFE Data Act builds on legislation passed by the House in 2009 but never acted upon in the Senate. Most importantly, it reflects the changing landscape of data breaches and data security since that time.

It's an upgraded, 2.0 version of data security legislation, encompassing many of the lessons learned in the aftermath of massive data breaches at Sony and Epsilon, which put more than 100 million consumer accounts at risk—and those are just the ones we know about.

As Subcommittee Chairman, protection from identity theft and online fraud is one of my top priorities. Just last week, Citigroup—which has the world's largest financial services network—revealed a security breach in which hackers obtained personal information from hundreds of thousands of accounts.

According to law enforcement officials, the hackers were able to gain access to customer names, account numbers and contact information such as e-mail addresses.

Yesterday, we learned that an external Web site operated by the Oak Ridge Nuclear Weapons Plant was victimized by a cyber attack, and earlier this week—the same group which claimed responsibility for attacks on Fox, PBS and Sony—also hacked the Senate's public Web site.

In recent years, carefully orchestrated cyber attacks—intended to obtain personal information about consumers, especially when it comes to their credit cards—have become one of the fastest growing criminal enterprises here in the United States and across the world.

The Federal Trade Commission estimates that nearly nine million Americans fall victim to identity theft every year, costing consumers and businesses billions of dollars annually. And the problem is only getting worse as these online attacks increase in frequency, sophistication and boldness.

As I have emphasized throughout our previous hearings, E-commerce is a vital and growing part of our economy. We should take steps to embrace and protect it—and that starts with robust cyber security.

Most importantly, consumers have a right to know when their personal information has been compromised, and companies and organizations have an overriding responsibility to promptly alert them. To that end, the SAFE Data Act:

Requires companies and other entities that hold personal information to establish and maintain appropriate security policies to prevent unauthorized acquisition of that data;

Requires the notification of law enforcement within 48 hours after discovery of a breach, unless that breach was an innocent or inadvertent breach unlikely to result in harm;

And it requires companies and other entities to begin notifying consumers 48 hours after taking steps to prevent further breach and determining who has to be notified.

The SAFE Data Act also gives the Federal Trade Commission authority over nonprofits for purposes of this act only. These organizations often posses a tremendous amount of consumer information, and they have been subjected to numerous breaches in the past. At the same time, we want to work with those affected, as well as the FTC, to make sure any new regulations are not burdensome for small businesses—especially during these difficult economic times.

In addition, we are granting the FTC authority to write rules that take into account the size and nature of the data that is being held online. Clearly, there are obvious differences between information brokers and local retail businesses—and the rules should reflect those differences.

The proposed legislation also requires all covered businesses to establish a data minimization plan providing for the elimination of consumers' personal data that is no longer necessary for business purposes or for other legal obligations.

And, finally, the SAFE Data Act preempts similar state laws to create uniform national standards for data security and data breach notification. We learned during our recent hearings that consumer notification is often hampered by the fact that companies must first determine their obligations under 47 different state regimes.

At the end of the day, I believe this legislation will greatly benefit consumers, businesses and the U.S. economy. Given the growing importance of e-commerce in nearly everything we do, we can no longer afford to sit back and do nothing. The time for action is now.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you, Madam Chairman.

I have said this at our previous hearing, and I want to repeat it today: Data security is not a partisan issue; it is something all of us should care about.

Last year, there were over 597 data breaches that affected over 12.3 million records. Last Congress, this committee worked together to pass with bipartisan support a data security bill introduced by Representative Rush. Our bill passed the House in December of 2009, but the Senate never took it up, so it was not completed.

The bill we are considering today is based on our bipartisan House bill from the last Congress. It contains important provisions that require companies to secure consumers' personal data and notify them in the case of breaches.

And I commend Chairman Bono Mack for using last year's bipartisan bill as a starting point. There are new provisions in the chair's draft that strengthen last Congress' bill. For example, the draft contains a potentially valuable new provision requiring companies to have plans to minimize personal data they retain on individuals.

Unfortunately, there are some changes in the bill that I fear weaken the bill rather than strengthen it. And this is a mistake and one I hope we can fix as we consider this legislation.

Let me raise some of the concerns I have: Under this legislation before us, Sony still would not have to notify its customers about its recent security breach. It did not restore the integrity of the data system for at least 43 days after Sony discovered the breach, and it still has not fully assessed the nature and scope of its breach. Notice is not required to the FTC and consumers under the draft until those steps have been completed.

Well, that is far too long. It does little good to notify consumers after their identities have already been stolen and make them wait such a long period of time.

This bill deletes key provisions on information brokers, which are companies that aggregate personal data about individuals and make a profit selling that personal information.

It adds unnecessary burdens to the Federal Trade Commission's rulemaking process, making it more difficult for new pieces of data to be deemed, quote, personal.

And there is significant ambiguity regarding the scope of personal information that a company is required to protect. Under this legislation companies, including an aggregator of data, are exempted from the requirements to safeguard personal information any time that same data can be found in various local county government buildings.

Furthermore, this draft creates an uneven playing field with potentially stronger data security and breach notification requirements for retailers than for nonbank financial institutions. There is no reason why financial institutions should be subject to smaller penalties for violations than retailers.

So I look at it as not a balanced bill overall. It gives businesses too many protections and consumers not enough. It preempts strong State laws and replaces them with a weak Federal one.

I hope these deficiencies in the bill can be fixed, and I want to work with the chair and other members of this committee to pass as effective a bill as possible, and I am looking forward to the promised stakeholder process. Today's hearing will give us a

chance to get further information about what a bill should and should not have in its details.

We have a chance to pass meaningful legislation that actually could make a positive effect on everyone, and we shouldn't pass up this opportunity.

I look forward to working with you, Madam Chair.

Mrs. BONO MACK. I thank the gentleman.

And the chair now recognizes Mr. Stearns for 2 minutes.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Thank you, Madam Chairman.

And thank you very much for calling this hearing. Obviously, as pointed out by yourself and the ranking member, Mr. Waxman, this is very important that we try to get a bipartisan support for this.

When I was chairman of this subcommittee, I introduced the Data Act in 2005, 6 years ago, established to protect unauthorized access to consumer data. This bill was co-sponsored by both sides when we marked it up, it was reported out of the full committee by unanimous consent.

Now, obviously, I would have preferred that we started with my bill, which is, I think, a bipartisan support product of a broad understanding of the security issues back in 2005. Now we are working with possibly a slightly different focused bill, which could be good, that addresses the recent breaches that occurred both in Sony and Epsilon. I think we have to be concerned that we not overreact based upon those two cases.

In both 2006 and 2009, there was bipartisan support for the Data Act that I had. Now we debate the SAFE Data Act, a bill that I am concerned has some very good points but also perhaps might be go too far in some other areas.

Obviously, I will work with the subcommittee, the chair lady, to improve the bill so it can pass with bipartisan support, like we have done in the past, so that the committee and the full House have an opportunity to vote on this. And so I look forward to the debate, and I look forward to our witnesses.

Thank you, Madam Chair.

Mrs. BONO MACK. I thank the gentleman.

The chair recognizes Mr. Olson for 1 minute.

Mr. OLSON. I thank the chair for her tenacious leadership in bringing forth this draft bill.

I think there is strong agreement that we need to move forward with Federal data security legislation. Support for Federal legislation has been bipartisan. My colleague from Florida, Mr. Stearns, put forth a data security bill in the 109th Congress, which Mr. Rush introduced in the 110th and 111th Congresses.

And now our chairwoman, Mrs. Bono Mack has put forth a bill in the 112th Congress.

I appreciate all of the efforts to help move us forward on this important issue, and I hope we can arrive at a truly bipartisan balanced bill that protects consumers without putting unnecessary burdens on companies or hindering important uses of data.

I look forward to continuing our discussion today and hope to be able to flesh out some issues that have been raised in testimony. I thank the chair and yield back my time.

Mrs. BONO MACK. I thank the gentleman.

And the chair recognizes Mr. Butterfield, the ranking member of the subcommittee, for 5 minutes.

OPENING STATEMENT OF HON. G.K. BUTTERFIELD, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Mr. BUTTERFIELD. I thank the chairman and apologize for being late.

The only thing I can say is don't try to go to Union Station at 10:00 on a Wednesday morning.

Madam Chairman, thank you for holding today's hearing on the Secure and Fortify Electronic Data Act. This bill includes some of the same provisions that we saw in H.R. 2221, which passed the House in the 111th Congress.

However, this draft also removes key consumer protection provisions that weaken the bill and make it less effective.

Americans' embrace of technology have served as the impetus for rapid growth of online businesses and services. I can buy a car without ever seeing it in person. I can pay my bills from one Web site, and I do it monthly. And I can even have all my data reside in a cloud, so it is accessible from absolutely anywhere.

In order for e-commerce to work, there must be data exchange between customer and businesses, including names, addresses, Social Security numbers, dates of birth and so on. The ability to conduct business in an online space is an amazing convenience. No one I know could do without it.

But the failure of some of these businesses to protect their own network infrastructure and the information demanded of their customers has led to opening—to an opening for small but not insignificant group of criminals to exploit and profit from the data these companies hold. And even those with strong security systems in place must be vigilant and adaptable to new threats.

During the 109th Congress and subsequent Congresses, members of this committee worked in a bipartisan fashion to develop the Data Accountability and Trust Act to address the issue of data security. In the last Congress, my friend and former chairman of the committee, subcommittee, Mr. Rush, introduced the data bill, which ultimately passed the House, but the Senate failed to act. That bill included special requirements for information brokers, including requiring brokers to submit security policies to the FTC and requiring an annual audit of broker security practices, among other things.

Striking those key provisions from the bill significantly weakens the consumer protections it is supposed to provide. Further, the draft bill defines personal information to exclude information that is publicly available. In doing so, the bill gives the green light to data aggregators to continue with business as usual without being required to have any safeguards in place to protect the data.

Madam Chairman, with over 2,500 data breaches having occurred since 2005, it is clear that the serious work of protecting

consumers' data is something that has taken a back seat in Congress for too long. A Federal standard is important. I will say that again: A Federal standard is important, and the SAFE Data Act is a start. I am sorry we are not starting with the text that passed the House in the last Congress.

Over the next few weeks, Madam Chairman, I hope you will work with me and my staff to strengthen this draft bill. Together we can ensure consumer protections while allowing businesses the flexibility to adapt their policies and procedures in today's rapidly evolving information age.

So thank you for having this hearing. I thank the commissioner for her presence today. And I think I might reserve my time. I am told that the gentlelady from Illinois is coming. She is not here. I yield back.

Mrs. BONO MACK. I thank the gentleman.

I just want to remind and reinforce to the entire panel that we intend fully on having a bipartisan product to the best of our ability and that will be our goal.

So now I would like to turn our focus to the witness table. We have two panels today. On the first panel, we are honored to have the Honorable Edith Ramirez, Commissioner at the FTC.

Thank you very much for being here today. You will be recognized for 5 minutes to summarize your statement. And just to—I am sure you are familiar with the time clock, it is yellow, green, red, kind of concept. When the light turns yellow, that means you have 1 minute to start your close.

So, at this point, we are happy to recognize you for your 5-minute statement.

Ms. RAMIREZ. Good morning.

Mrs. BONO MACK. And, please, remember to turn your microphone on.

STATEMENT OF EDITH RAMIREZ, COMMISSIONER, FEDERAL TRADE COMMISSION

Ms. RAMIREZ. Good morning.

Chairman Bono Mack, Ranking Members Butterfield and Waxman, and members of the subcommittee, I am Edith Ramirez, a Commissioner of the Federal Trade Commission. I appreciate the opportunity to present the commission's testimony on data security.

I want to thank you, Chairman Bono Mack, and the committee for your leadership on this important issue.

Before I continue I would like to note that my written testimony represents the views of the Federal Trade Commission, but my oral remarks and responses to questions are my own and may not reflect the views of the commission as a whole or of other commissioners.

As the Nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. If companies do not protect the personal information they collect and store, information could fall into the wrong hands, resulting in fraud and other harm and consumers could lose confidence in the marketplace.

Although data security has recently been in the news, this is not a new priority for the FTC. To the contrary, for a decade, the FTC

has undertaken substantial efforts to promote data security in the private sector through law enforcement, education, policy initiatives, and recommendations to Congress to enact legislation in this area.

Since 2001, the FTC has brought 34 cases charging that businesses failed to appropriately protect consumers' personal information. This includes a final settlement the commission is announcing today against Ceridian Corporation, a large payroll processor. Ceridian's clients upload their employee sensitive information, including Social Security numbers and bank account numbers, which are stored on Ceridian's network. The FTC's complaint charged that Ceridian didn't maintain reasonable safeguards to protect this employee information. As a result, a hacker was able to gain access to it.

The FTC's order requires Ceridian to implement a comprehensive data security program and obtain independent audits for 20 years.

The commission also promotes better data security through consumer and business education. For example, on the consumer education front, we sponsor OnGuard Online, a Web site to educate consumers about basic computer security. Since its launch in 2005, there have been over 14 million unique visits to OnGuard Online and its Spanish language counterpart, Alerta en Linea.

We also conduct outreach to businesses, especially small businesses, to provide practical advice about data security. The commission also engages in policy initiatives to promote data security.

Last December, FTC staff issued a preliminary report proposing a new framework to improve consumer privacy and data protection. Among other things, the report advocates privacy by design, which includes several principles essential to data security. First, companies, no matter what their size, should employ reasonable, physical, technical and administrative safeguards to protect information about consumers. Second, companies should collect only that consumer information for which they have a legitimate business need. Third, businesses should retain data only as long as necessary to fulfill the business purpose for which it was collected and should promptly and securely dispose of data they no longer need.

As to legislation, the commission generally supports Federal legislation, similar to your draft proposal, that would impose data security standards on companies and require companies in appropriate circumstances to notify consumers when there is a security breach. Reasonable security practices are critical to preventing data breaches, and if a breach occurs, prompt notification to consumers in appropriate circumstances can mitigate harm such as ID theft. For instance, in the case of a breach of Social Security numbers, notified consumers can request that fraud alerts be placed in their credit files, obtain copies of their credit reports and scrutinize their monthly account statements.

The commission is pleased that your draft legislation includes civil penalty authority to deter violations, APA authority for rulemaking and jurisdiction over nonprofit entities for data security purposes. I would also like to note that both your draft legislation and the commission staff's recent privacy report underscore the importance of data minimization to sound data security practices.

The FTC looks forward to working with this committee as it moves forward on the SAFE Data Act. Thank you, again, for inviting me to be here and for your leadership on these important issues, and I am pleased to answer any of your questions.

[The prepared statement of Ms. Ramirez follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

Data Security

Before the

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

UNITED STATES HOUSE OF REPRESENTATIVES

Washington, D.C.

June 15, 2011

I. INTRODUCTION

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, I am Edith Ramirez, a Commissioner of the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on data security, and the Commission thanks you for your leadership on data security issues affecting today's consumers.[1]

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector and has brought 34 law enforcement actions against businesses that allegedly failed to protect consumers' personal information appropriately.[2] Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private sector through law enforcement, education, and policy initiatives. Just today, the Commission finalized two data security orders, and next month, the Commission will be hosting a forum to explore the issue of identity theft targeting children. This testimony provides an overview of the Commission's efforts and reiterates the Commission's unanimous,

---

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] In addition to these data security cases, in the last fifteen years, the FTC has brought numerous cases to protect consumer privacy including 64 cases against companies for improperly calling consumers on the Do Not Call registry; 86 cases against companies for violating the Fair Credit Reporting Act ("FCRA"); 96 spam cases; 15 spyware cases; and 16 cases against companies for violating the Children's Online Privacy Protection Act.

bipartisan support for legislation that would require companies to implement reasonable data security policies and procedures and, in the appropriate circumstances, provide notification to consumers when there is a security breach.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

To promote data security, the Commission enforces several laws and rules that impose obligations on businesses that possess consumer data. The Commission's Safeguards Rule under the Gramm-Leach-Bliley Act ("GLB Act"), for example, provides data security requirements for financial institutions,[3] and the Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information, and imposes safe disposal obligations on entities that maintain consumer report information.[4] In addition, the Commission enforces the FTC Act's proscription against unfair or deceptive acts or practices in cases where a business makes false or misleading data security claims or where its failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.[5]

Since 2001, the Commission has used its authority under these laws to bring 34 cases against businesses that allegedly failed to protect consumers' personal information

---

[3] 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b). The Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Office of Thrift Supervision, Secretary of the Treasury, and state insurance authorities have promulgated comparable safeguards requirements for the entities they regulate.

[4] 15 U.S.C. §§ 1681e, 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

[5] 15 U.S.C. § 45(a).

appropriately.[6] As noted above, just today, the Commission announced that it had given final approval to consent orders in data security cases involving Ceridian Corporation and Lookout Services, Inc. Ceridian is a large payroll processing company that maintains highly-sensitive payroll information.[7] In December 2009, as a result of Ceridian's alleged failures to adequately protect its data, an intruder was able to hack into Ceridian's payroll processing system and compromise the personal information – including Social Security numbers and financial account

---

[6] *See Lookout Servs.,Inc.*, File No. 1023076 (June 15, 2011) (consent order); *Ceridian Corp.*, File No. 1023160 (June 15, 2011) (consent order); *SettlementOne Credit Corp.*, File No. 082 3208, *ACRAnet, Inc.*, File No. 092 3088, and *Fajilan & Assocs., Inc.*, File No. 092 3089 (Feb. 3, 2011) (consent orders approved for public comment); *Rite Aid Corp.*, File No. 072-3121 (July 27, 2010) (consent order); *Twitter, Inc.*, File No. 092-3093 (June 24, 2010) (consent order); *Dave & Buster's, Inc.*, FTC Docket No. C-4291 (May 20, 2010) (consent order); *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-NVW (D. Ariz. Mar. 15. 2010) (stipulated order); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198-JTC (N.D. Ga. Oct. 14, 2009) (stipulated order); *James B. Nutter & Co.*, FTC Docket No. C-4258 (June 12, 2009) (consent order); *United States v. Rental Research Servs.*, No. 0:09-CV-00524 (D. Minn. Mar. 6, 2009) (stipulated order); *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 29, 2009) (stipulated order); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008) (stipulated order); *United States v. American United Mortg.*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007) (stipulated order); *CVS Caremark Corp.*, FTC Docket No. C-4259 (Jun. 18, 2009) (consent order); *Genica Corp.*, FTC Docket No. C-4252 (Mar. 16, 2009) (consent order); *Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008) (consent order); *The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008) (consent order); *Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008) (consent order); *Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (consent order); *Goal Fin'l., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008) (consent order); *Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007) (consent order); *CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006) (consent order); *Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006) (consent order); *DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006) (consent order); *Superior Mortg. Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) (consent order); *BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005) (consent order); *Nationwide Mortg. Group, Inc.*, FTC Docket No. C-9319 (Apr. 12, 2005) (consent order); *Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (consent order); *Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005) (consent order); *MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (consent order); *Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003) (consent order); *Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (consent order).

[7] *Ceridian Corp.*, File No. 1023160 (June 15, 2011) (consent order).

numbers – of approximately 28,000 employees of Ceridian's small business customers.

Lookout Services offers a web-application to assist employers in meeting federal requirements to verify their employees' eligibility to work in the United States.[8] Within this application, Lookout maintains highly-sensitive information provided by employees, including Social Security numbers, dates of birth, passport numbers, alien registration numbers, driver's license numbers, and military identification numbers. In October and December of 2009, due to the company's alleged weak authentication practices and web application vulnerabilities, an employee of a Lookout customer obtained unauthorized access to the entire Lookout customer database.

In both cases, the Commission alleged that the companies did not maintain reasonable safeguards for the highly-sensitive information they maintained. Specifically, the Commission alleged that, among other things, both companies failed to adequately assess the vulnerability of their web applications and networks to commonly known or reasonably foreseeable attacks. The orders require the companies to implement a comprehensive data security program and obtain independent audits for 20 years.

In addition, earlier this year, the Commission brought actions against three credit report resellers, alleging violations of the FCRA, the FTC Act, and the Safeguards Rule.[9] Due to their lack of information security policies and procedures, the respondents allegedly allowed clients without basic security measures, such as firewalls and updated antivirus software, to access

---

[8] *Lookout Servs., Inc.*, File No. 1023076 (June 15, 2011) (consent order).

[9] *SettlementOne Credit Corp.*, File No. 082 3208; *ACRAnet, Inc.*, File No. 092 3088; *Fajilan & Assoc., Inc.*, File No. 092 3089 (Feb. 3, 2011) (consent orders approved for public comment).

sensitive consumer reports through an online portal. This failure enabled hackers to access more than 1,800 credit reports without authorization. As with *Ceridian* and *Lookout*, the settlements require each company, among other things, to have comprehensive information security programs in place to protect consumers' personal information.

B. Education

The Commission also promotes better data security practices through extensive consumer and business education. On the consumer education front, the Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security.[10] OnGuard Online was developed in partnership with other government agencies and the technology sector. Since its launch in 2005, OnGuard Online and its Spanish-language counterpart Alerta en Línea[11] have recorded more than 14 million unique visits.

In addition, the Commission has engaged in wide-ranging efforts to educate consumers about identity theft, one of the harms that could result if their data is not adequately protected. For example, the FTC's identity theft primer[12] and victim recovery guide[13] are widely available in print and online. Since 2000, the Commission has distributed more than 10 million copies of the two publications and recorded over 5 million visits to the Web versions. In addition, in February 2008, the U.S. Postal Service – in cooperation with the FTC – sent copies of the

---

[10] *See* http://www.onguardonline.gov.

[11] *See* http://www.alertaenlinea.gov.

[12] *Avoid ID Theft: Deter, Detect, Defend, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.htm.

[13] *Take Charge: Fighting Back Against Identity Theft, available at* http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm.

Commission's identity theft consumer education materials to more than 146 million residences and businesses in the United States. Moreover, the Commission maintains a telephone hotline and dedicated website to assist identity theft victims and collect their complaints, through which approximately 20,000 consumers contact the FTC every week.

The Commission also partners with local businesses, community groups, and members of Congress to educate their employees, communities, and constituencies. For example, the Commission has launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend," which contains a consumer education kit that includes direct-to-consumer brochures, training materials, presentation slides, and videos for use by such groups. Since the campaign launch in 2006, the FTC has distributed nearly 110,000 consumer education kits and over 100,000 "Protect Your Identity Day" kits.[14]

The Commission directs its outreach to businesses as well. The FTC widely disseminates its business guide on data security, along with an online tutorial based on the guide.[15] These resources are designed to provide diverse businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. The Commission has also released articles directed towards a non-legal audience regarding basic data security issues for businesses.[16] The FTC creates business educational materials on specific topics – such as the risks associated with P2P file-sharing programs and

---

[14] *See* www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt06.pdf.

[15] *See* http://www.ftc.gov/infosecurity.

[16] *See* http://business.ftc.gov/privacy-and-security.

companies' obligations to protect consumer and employee information from these risks[17] and how to properly secure and dispose of information on digital copiers.[18]

C. Policy

The Commission also undertakes wide-ranging policy initiatives to promote data security. This testimony describes two such initiatives – the recent Privacy Roundtables and accompanying preliminary staff report as well as an upcoming forum on child identity theft.

1. Privacy Roundtables and Preliminary Staff Report

In December 2009, February 2010, and March 2010, the FTC convened three public roundtables to explore issues surrounding consumer privacy.[19] Panelists at the roundtables repeatedly noted the importance of data security as an important component of protecting consumers' privacy. Many participants stated that companies should incorporate data security into their everyday business practices, particularly in today's technological age. For example, participants noted the increasing importance of data security in a world where cloud computing enables companies to collect and store vast amounts of data at little cost.[20]

Based on these roundtable discussions, staff issued a preliminary privacy report in

---

[17] *See Peer-to-Peer File Sharing: A Guide for Business, available at* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

[18] *See* http://business.ftc.gov/documents/bus43-copier-data-security.

[19] *See generally* FTC Exploring Privacy web page, http://www.ftc.gov/bcp/workshops/privacyroundtables.

[20] *See, e.g.,* Privacy Roundtable, Transcript of January 28, 2010, at 182, Remarks of Harriet Pearson, IBM (noting the importance of data security as an issue for new computing models, including cloud computing).

December 2010,[21] which proposed and solicited comment on a new framework to guide policymakers and industry as they consider further steps to improve consumer privacy protection. The proposed framework incorporates the principles of privacy by design, simplified privacy choices for consumers, and improved transparency of privacy practices for consumers. In the context of data security, the principle of "privacy by design" is especially important. Indeed, consumers should not be expected to understand and evaluate the technical details of a company's data security plan; rather, reasonable security should be incorporated into the company's business practices.

As the staff report notes, privacy by design includes several substantive components related to data security. First, companies that maintain information about consumers should employ reasonable safeguards – including physical, technical, and administrative safeguards – to protect that information. The level of security required depends on the sensitivity of the data, the size and nature of a company's business operations, and the types of risks a company faces. Second, companies should collect only information for which they have a legitimate business need. Because the collection and maintenance of large amounts of data increases the risk of unauthorized access to the data and the potential harm that could result, reasonable data collection practices are a critical component of sound data security. Third, businesses should retain data only as long as necessary to fulfill the business purposes for which it was collected and should promptly and securely dispose of data for which they no longer have a business need.

---

[21] *See Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners Kovacic and Rosch issued concurring statements available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at Appendices D and E, respectively.

While old data may not be valuable to a particular company, it can be highly valuable to an identity thief.

In addition to these substantive principles, the staff report recommends that companies implement and enforce privacy procedures – including appropriate data security – throughout their organizations. This includes assigning personnel to oversee such issues, training employees, and assessing and addressing risks to privacy and security.

2. Child Identity Theft Forum

Along with periodically conducting policy reviews of privacy and security issues generally, the Commission also hosts workshops to study and publicize more specific issues. One issue that has been in the news recently is identity theft targeting children.[22] For a variety of reasons – including poor safeguards for protecting children's data – identity thieves can get access to children's Social Security numbers. These criminals may deliberately use a child's Social Security number, or fabricate a Social Security number that coincidentally has been assigned to a child, in order to obtain employment, apply for government benefits, open new accounts, or apply for car loans or mortgages. Child identity theft is especially pernicious because the theft may not be detected until the child becomes an adult and seeks employment or applies for a loan.

To address these challenges, Commission staff, along with the Department of Justice's

---

[22] *See e.g.*, Richard Power, Carnegie Mellon Cylab, *Child Identity Theft, New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers* (2011), *available at* http://www.cyblog.cylab.cmu.edu/2011/03/child-identity-theft.html; Children's Advocacy Institute, *The Fleecing of Foster Children: How We Confiscate Their Assets and Undermine Their Financial Security* (2011), *available at* http://www.caichildlaw.org/Misc/Fleecing_Report_Final_HR.pdf.

Office of Victims of Crime, will host a forum on July 12, 2011.[23] Participants, including educators, child advocates, and representatives of various governmental agencies and the private sector, will discuss how to improve the security of children's data in various contexts, including the education system as well as the foster care system, where children may be particularly susceptible to identity theft. The goal of the forum is to develop ways to effectively advise parents on how to avoid child identity theft, how to protect children's personal data, and how to help parents of victims, and young adults who were victimized as children, recover from the crime.

III. DATA SECURITY LEGISLATION

Finally, the Commission would like to offer a few comments on the discussion draft of Chairman Bono Mack's proposed data security bill. As a general matter, the Commission reiterates its general support for federal legislation that would (1) impose data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.[24] Companies' implementation of reasonable security is important for protecting consumers' data from identity theft and other harms. And if a breach occurs, prompt notification to consumers in appropriate circumstances can mitigate any such

---

[23] *See* http://www.ftc.gov/bcp/workshops/stolenfutures.

[24] *See e.g.*, Prepared Statement of the Federal Trade Commission, *Protecting Social Security Numbers From Identity Theft*, Before the Subcommittee on Social Security of the House Committee on Ways and Means, 112th Cong., April 13, 2011, *available at* http://ftc.gov/os/testimony/110411ssn-idtheft.pdf (citing the Commission's support for data security and breach notification standards); FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; and President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

harm.[25] For example, in the case of a breach of Social Security numbers, notified consumers can request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves. The Commission appreciates that the discussion draft accomplishes these goals.

The Commission further appreciates the discussion draft's inclusion of several specific elements. First, the discussion draft provides the agency with rulemaking authority in several areas, and authorizes it to use the standard notice and comment procedures required by the Administrative Procedure Act in lieu of the current rulemaking procedures prescribed by Section 18 of the FTC Act (often referred to as "Magnuson-Moss" rulemaking). The Commission supports this provision, as effective consumer protection requires that the Commission be able to promulgate these rules in a more timely and efficient manner. Second, the Commission supports the inclusion of a provision authorizing the agency to obtain civil penalties for violations.[26] Civil

---

[25] Indeed, various states have already passed data breach notification laws that require companies to notify affected consumers in the event of a data breach. These laws have increased public awareness of data security issues and related harms, as well as data security issues at specific companies. *See, e.g.,* Federal Trade Commission Report, *Security in Numbers: SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, *Security Breach Notification Laws: Views from Chief Security Officers* (Dec. 2007), *available at* http://www.law.berkeley.edu/files/cso_study.pdf. Breach notification at the federal level would extend notification nationwide and accomplish similar goals.

[26] *See, e.g.,* Prepared Statement of the Federal Trade Commission Before Subcomm. on Consumer Protection, Product Safety & Insurance of the S. Comm. on Commerce, Science & Transportation, 111th Cong. (Sep. 22, 2010), *available at* http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf; Prepared Statement of the Federal Trade Commission Before the Subcomm. on Interstate Commerce, Trade, and Tourism of the S. Comm. on Commerce, Science, and Transportation Committee, 110th Cong. (Sep. 12, 2007) *available at* http://www.ftc.gov/os/testimony/070912reauthorizationtestimony.pdf; Prepared Statement of the Federal Trade Commission Before the S. Comm. on Commerce, Science, and Transportation, 110th Cong. (Apr. 10, 2007), *available at* http://www.ftc.gov/os/testimony/P040101FY2008BudgetandOngoingConsumerProtectionandCo

penalties are particularly important in areas such as data security, where the Commission's traditional equitable remedies – including consumer restitution and disgorgement – may be impractical or not optimally effective. Third, the Commission continues to support legislative provisions that would authorize the Commission to sue non-profit entities for data security violations, and appreciates the draft proposal's inclusion of such provisions.[27] Finally, the Commission notes that the recent Commission staff report takes the same position as the discussion draft that data minimization is an important component of data security.

The Commission is ready to work with this Committee as it develops and considers data security legislation.

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on data security. We remain committed to promoting data security and look forward to continuing to work with the Subcommittee on this important issue.

---

mpetitionProgramsTestimonySenate04102007.pdf; *see also* FTC Report, *Recommendations on Social Security Number Use in the Private Sector* (Dec. 2008), *available at* http://www.ftc.gov/opa/2008/12/ssnreport.shtm.

[27] The Commission has authority to sue sham non-profits under existing law. *See, e.g.*, http://www.ftc.gov/opa/2009/05/charityfraud.shtm.

Mrs. BONO MACK. Thank you very much.

The chair now recognizes herself for 5 minutes for questioning. The first question I have, you state the commission's support for prompt notice to consumers. I think it is the crux of what we are all about here. What do you consider prompt, and do you think the consumer notification requirement in the legislation is quick enough?

Ms. RAMIREZ. I believe that notification needs to be provided as soon as practicable. I do have some concerns about the provision relating to notification in the draft bill. And let me highlight the two key concerns. My first concern is that the bill requires that there be a risk assessment performed, and then, at the conclusion of that risk assessment, a company is then obligated to provide notification to consumers and to the FTC 48 hours, within 48 hours following that.

My concern is that the requirement, that there is no deadline on which to complete a risk assessment, and therefore, that could take an indefinite amount of time. Without there being some type of limit that is placed on that, I think it places consumers at significant risk.

Another concern that we have is that there is also no time limit that is placed in connection with law enforcement, that it could also be an open-ended deadline that could delay prompt notification to consumers. And again, there ought to be some form of a cut-off period to ensure that consumers received appropriate notification within an appropriate amount of time so that they can take steps to mitigate any harm that may result from a data breach.

I would also like to emphasize that providing prompt notice to the FTC is also very critical, and in our view, notice to the FTC should be provided at the same time that it is provided to other law enforcement agencies.

Mrs. BONO MACK. Thank you.

And the FTC has experience under Gramm-Leach-Bliley with the implementation of the safeguards rule for financial institutions under its jurisdiction. The FTC also provided comprehensive guidance for entities to understand how they can comply with the rule. Do those guidelines provide a sufficient indication of the rules for data security the FTC would write under Section 2 of this legislation?

Ms. RAMIREZ. I think they do provide good guidance to companies. In addition to the to particular enforcement matters and consent orders that the commission makes public, the commission provision many, many different resources online to companies so that they can take appropriate measures to adequately protect consumer information.

Mrs. BONO MACK. So, under Section 2 security requirements of the draft legislation, does the FTC have the latitude to write rules that take into account the different types of entities, their level of sophistication and the amount of type of information they hold?

Ms. RAMIREZ. It does. And we appreciate that authority being provided to the FTC to promulgate rules detailing those.

Mrs. BONO MACK. Do you envision writing different rules or different guidance to address the concerns that a one-size-fits-all approach is not appropriate?

Ms. RAMIREZ. During the rulemaking process, we would be seeking input from stakeholders and fashioning rules that, in light of the input that we received, that we believe would be appropriate to protect consumer information.

Mrs. BONO MACK. So do you see different standards, then, for information brokers and small nonprofits, for example?

Ms. RAMIREZ. We believe that companies, no matter what the size, need to provide solid and good data security measures. At the same time, the standards that the FTC employees in its enforcement work is a reasonableness standard, so we do take into account the size of a company, the nature of the information that has been placed at risk and other factors that may weigh in on that calculus.

Mrs. BONO MACK. Since we first started this process 6 years ago, 46 State laws have emerged. Nearly every one of them, including California, have exemptions from the definition of personal information for information made publicly available by the government and, in some cases, information made public by the media.

The exemption included in this draft is confined to information made publicly available by the government.

Have you seen any problems of unlawful activity associated with the publicly available information?

Ms. RAMIREZ. Yes. We do have concerns about there being an exemption for public, for all public information. The difficulty is that these days there are data brokers that collect information that in the past, one would have to go to very significant measures to collect. You would have to go—you could go to the courthouse; you could collect information through other means. But data aggregators then aggregate this information and when the information, which may very well be public, is then collected, gathered and aggregated, it can then pose very unique privacy challenges. So we do have concerns about there not being a mechanism to address those issues relating to data brokers.

Mrs. BONO MACK. You said privacy challenges. Do you mean security challenges?

Ms. RAMIREZ. Security challenges.

Mrs. BONO MACK. Thank you. All right.

I yield back the 5 seconds of my time.

And the chair recognizes Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. Thank you very much.

Thank you, Commissioner. The Republican discussion draft makes a change from H.R. 2221 to the definition of personal information. That seems like a simple and minor change, but it actually is not. It excludes public record information from the definition of personal information.

Given that technology has made access to an aggregation of numerous of types of records very cheap and easy the consequences of this change are quite significant. Before it became cheap and easy to store vast amounts of this information in one place, no one thought about going out and collecting these records. To see these records, you had to, as you said a moment ago, go from town hall to town hall or courthouse to courthouse and look at them one at a time. But now, millions and millions of records regarding millions

of our constituents are being kept on servers usually belonging to information brokers.

If you are a criminal wanting to do harm to lots of people in one swoop, the Republican discussion draft will be an advantage to you. This collection and aggregation in one place has changed the value of this information and its susceptibility to criminal misuse, and it concerns me that this draft bill leaves this information unprotected.

Because of the change to the definition of personal information to exclude public record information, there is no longer an obligation to provide any protection at all for this information.

Have I said it correctly, Commissioner, or have I misspoken?

Ms. RAMIREZ. We agree with that concern yes.

Mr. BUTTERFIELD. Do you believe that just because that information could have been collected elsewhere, a covered person should be relieved of the obligation to protect its information when they collect and aggregate the information in one place and make it more valuable and potentially more dangerous? Please help me with that.

Ms. RAMIREZ. I believe that information, even if it is public information, if it is personal information of the consumer, that information ought to be protected, and there ought to be appropriate data security measures in place to protect it.

Mr. BUTTERFIELD. All right.

I want to take your attention to notification. Do you believe notification to consumers should also be required for breaches involving this kind of information?

Ms. RAMIREZ. Yes.

Mr. BUTTERFIELD. The Republican discussion draft, like H.R. 2221 before it, provides the FTC, your commission, with the ability to modify the definition of personal information. Only information that is within the meaning of that term is covered by the bill's data security and breach notification requirements.

But unlike 2221, the discussion draft seems to set up an overly burdensome and unclear process for modifying that definition. If the FTC wanted to change the definition for the purposes of either the data security or notification sections, it would have to find, among other things, that modification would not unreasonably impede Internet or other technological innovation or otherwise adversely affect interstate commerce, end of quote.

Question, do you believe this language regarding impediments to innovation provides the FTC with much of a clear standard against which to determine whether a modification is appropriate?

Ms. RAMIREZ. I do have concerns about the standards that are imposed. In addition to the limitation on changes to the definition that could impede innovation, as you mentioned, it also requires that the commission only make a change when there is a technological change at issue, and that is in connection with the data security piece of the proposed bill. So that does raise concerns because we feel there are issues with the definition of personal information. It is too narrow, and we would not be able to address those concerns.

Mr. BUTTERFIELD. Well, what would you do? How would you make that determination if you were called upon to do so?

Ms. RAMIREZ. Well, again, we would want to work with the committee on establishing an appropriate limitation. But let me articulate a couple of concerns that we have with the personal information limitation, in addition to the public records exemption.

Two things: First, we believe that the financial, that the provision focuses solely on financial related information and doesn't take into account, for instance, other information that would be sensitive to a consumer. For instance, health information that would not otherwise be protected under HIPAA would not be covered by the language in the draft bill. So that would be a concern that we would not be able to address through the rulemaking that is provided in the draft bill.

Mr. BUTTERFIELD. And what about the language that speaks to impeding innovation? I don't know how you define that.

Ms. RAMIREZ. That would be a difficult standard also to apply, and so, arguably, rules by the commission could be challenged by parties arguing that the change in definition could impede the growth and make other arguments, so it would place an undue burden, we believe, on the commission.

Mr. BUTTERFIELD. Thank you. I yield back.

Mrs. BONO MACK. I thank the gentleman and want to thank him very much for pointing out the few bracketed points in the legislation where we specifically bracketed them because we, too, have questions in the draft, so I appreciate the clarification in your input, and I appreciate the gentleman taking the opportunity to raise that.

The chair recognizes Mr. Stearns for 5 minutes.

Mr. STEARNS. Thank you, Madam Chair.

One thing I just thought we would clear, that I think the Federal preemptions that it had in my bill in 2005 and the bill that passed in the Rush haven't changed. So as I understand, I just want to ask counsel, is that true that the Federal preemption have not changed, so that any criticism that would be brought from that side because of that, that they haven't changed at all?

The COUNSEL. Yes, sir, that is correct.

Mr. STEARNS. Ms. Ramirez, as you are aware, in the bill, the Federal Trade Commission has the authority to change the very fundamental definition of personally identifiable information. So this gives you this broad latitude, I think a lot of us are a little concerned about. Do you think there is an opportunity where the Federal Trade Commission under any circumstances would trigger the need for them to alter, to update, to change that basic definition how it is currently drafted in the bill now, because you have got this definition that people understand in the bill, yet you have the authority to change it? Under what circumstances would you change it, and perhaps you could explain what would cause it?

Ms. RAMIREZ. One circumstance that could arise is there could be changes in technology that could require additional information being needed.

Mr. STEARNS. But isn't personal identifiable information pretty much policy-neutral because it represents an understanding of the privacy of the individual?

Ms. RAMIREZ. I think the precise scope may be hard to define. But the commission is absolutely willing to work with the com-

mittee to come up with a definition that would meet every one and satisfy everyone's concern. The current condition we believe is to narrow. We also believe that the ruling provided is too limited.

I will say that the rulemaking process that the commission employs is a process by which we do seek input from stakeholders. And we believe that through that rulemaking process, we will be able to address any need for change, at the same time taking into account any concerns that you and others may have, Congressman.

Mr. STEARNS. Well, I think that probably if I was in industry, I would be concerned that the government, the Congress, is turning over this power to you and you might make these changes without a comment period. There might be changes that would affect a business that would make it much more difficult.

Let me go on to my second question. In the bill, they added data minimization provisions. Now, this is something new from my bill, and also it is new from the Rush bill. How do you see this provision playing out? For members and people who don't understand, this is basically forcing industry to get rid of information that perhaps they would like to keep. It is not a decision they make, it is a mandated mandate, which is included in the bill, as I understand it. So I guess the question is, how do you see this provision playing out, and what role do you believe, if any, the FTC should have in ensuring that companies are complying? So you have this mandate; the companies might not agree, so if they don't do it, how are you going to check it, and how are you going to make them comply?

Ms. RAMIREZ. What the commission advocates is that companies only retain information that they have a legitimate business need to retain.

Mr. STEARNS. And who determines that?

Ms. RAMIREZ. And that they also only retain it for the time period they need it. I think we would apply a reasonableness standard.

Mr. STEARNS. What kind of standard?

Ms. RAMIREZ. A reasonableness standard, which is a standard that the FTC has employed throughout the course of its enforcement in this arena.

Mr. STEARNS. So this reasonable standard in your mind is been pretty much established at the FTC so everybody in industry would understand today what it is?

Ms. RAMIREZ. What I am saying is that the standard that would be applied would be a reasonableness standard, and I believe—it is an issue that may need to be fleshed out. And again, the commission is willing to work with the committee in order to do that. Any rulemaking that does take place would entail a comment period, absolutely entail a comment period. I believe that the FTC has a very solid track record in terms of its rulemaking. So I think this is an area, again, that the standard that the FTC has always applied in the area of data security is one of reasonableness, taking into account the nature of the information, how sensitive it is, the potential risks to consumer. So it would be a reasonableness standard that would be applied.

Mr. STEARNS. Do you think that Congress should set the broad outline for this data minimization provision and not give it any au-

thority to the FTC, or do you think you need to have that authority to make that decision?

Ms. RAMIREZ. I think it would be appropriate to give authority and flexibility to the FTC to provide additional guidance to companies as to how to effectuate those requirements.

Mr. STEARNS. Thank you.

Mrs. BONO MACK. The gentleman's time is expired. The chair recognizes Mr. Waxman for 5 minutes.

Mr. WAXMAN. Thank you, Madam Chair. Again, looking at this draft bill, I have some questions, so that we can get your input on it. As I look at the draft bill, there is a notice that must be given to the Federal Trade Commission and the consumers when there has been an electronic data breach. But it is only required after the covered person, the people who—a company who has the identifying information has done certain things in connection with the breach. The covered person must, one, assess the nature and scope of the breach, that makes sense, take steps to further prevent breach orunauthorized disclosure, and then, three, restore the integrity of the data system. Those clearly are the priorities for the company itself.

After they have done all that, the covered person must determine the risk to the consumer. And after they have reached that conclusion, within 48 hours, they are supposed to give the notice to the FTC and the consumer. But there is no limit in this draft bill for how long a person can take to complete steps one, two and three. There is just no limit. The covered person, company, knows about a breach, could take a week, a year, maybe 5 years and then, within 48 hours of that, provide notice to the Federal Trade Commission and the consumers.

The bill from the last Congress included an outer limit of 60 days from the discovery of the breach to provide notice of the breach. That outer limit has been dropped from this discussion draft. If we were to include an outer limit, how long should that limit be, in your opinion.

Ms. RAMIREZ. In my view, and the commission's view, is that the time for notification should be as soon as practicably possible. That may differ depending on the circumstances. I believe that 60 days should be at most an outer limit. Again, our view is that the sooner, the better. The sooner the notice is provided, the sooner that a consumer can take appropriate steps to protect and try to mitigate any harm that may result from a breach.

I don't believe there is a particular number that I can give you sitting here today because it may depend on the circumstances, the nature of the breach, the size of the company, but I would say that 60 days would be at most an outer limit.

Mr. WAXMAN. Sixty days would be an outer limit, but as soon as practicable?

Ms. RAMIREZ. Yes.

Mr. WAXMAN. That the information should go to the consumer that their identity has been compromised?

Ms. RAMIREZ. That is correct.

Mr. WAXMAN. A security leak. Thank you for that.

The discussion draft provides an exemption from the bill's data security requirements for entities that are subject to data security

requirements under different bills, the Gramm-Leach-Bliley or the Health Insurance Portability and Accountability Act, for any activities governed by GLB and HIPAA. Now, this is a departure from last year's bill.

Last year's bill only said that compliance with these two other statutes meant you were in compliance with the requirements of this legislation as it was drafted, provided that the requirements of GLB and HIPAA were similar or greater than those required under last year's bill. The language was not phrased as exemption for entities subject to FTC jurisdiction but rather as an alternative means of compliance.

It is unclear to me whether under the draft bill, the Federal Trade Commission maintains the ability to enforce any data security requirements against those entities or if the safeguards in those other laws must meet or exceed those in the discussion draft. Do you believe that this exemption could potentially limit the Federal Trade Commission's enforcement abilities with respect to entities subject to the other two statutes, those other two statutes, and could you explain your answer to that?

Ms. RAMIREZ. Under my reading of the bill, I do believe that it creates, potentially creates a gap in authority, because it does exempt entities that are subject to FTC jurisdiction from having breached notification requirements which are not required under Gramm-Leach-Bliley. So that is a concern about there being a potential gap in authority.

Mr. WAXMAN. And do you believe this exemption could potentially lead to a disparity in the security requirements for nonbank financial institutions and everyone else under the——

Ms. RAMIREZ. I do.

Mr. WAXMAN. And what is your understanding of the effect of the phrase "any activities governed by GLB or HIPAA" on the scope of this exemption? What is the Gramm-Leach-Bliley activity, is that just issuing privacy notices? Is that following the FTC's safeguard rule, or is that marketing?

Ms. RAMIREZ. Again, that activity-based exemption, it is a little bit unclear exactly how broadly it might be interpreted. But I think that the key point is that it does create a disparity between the obligations of certain financial institutions so that it is a concern about in connection with the authority that is provided.

Mr. WAXMAN. Thank you.

Madam Chair, I just want to point this out as an area where we need to work together to make sure that there is no ambiguity or poor drafting that would undermine what we are trying to do.

Mrs. BONO MACK. I thank the gentleman very much. I agree with his questioning and agree with his assessment about where we can fortify the bill, and I look forward to working with you on that.

And the chair is happy to recognize Mr. Olson for 5 minutes.

Mr. OLSON. I thank the chair.

Commissioner Ramirez, welcome. Thank you for your time today. As you know the SAFE Data Act would require an entity to begin to notify as promptly as possible, and that is a quote, individuals whose personal information was acquired or assessed in a breach following an assessment, and a notification should be based on risk

of harm, not just on the fact that a breach had occurred. Otherwise, we may find ourselves in a situation where consumers are flooded with notices by companies, become desensitized, and then may not take action to protect themselves when there is a real risk due to a significant breach where personal identifiable information was stolen, and identity theft could occur.

As currently drafted this legislation standard for risk is, quote, reasonable risk of harm. In response to my colleague Congressman Stearns' questions, you said that that is the standard that the FTC supports. Do you think consumers would be better served in the long run if the standard were changed to, "significant risk of harm"? And what in your opinion is the difference between a reasonable risk of harm and a significant risk of harm?

Ms. RAMIREZ. I don't think that consumers would be better served if the standard were to be elevated to a significant risk. I think the key objective, as I understand it, of the draft bill is to ensure that consumers are appropriately protected if there is a breach. And my concern would be that by imposing a higher standard, that key objective would be undermined.

So I think it is appropriate to apply a reasonableness standard. But my fear is that by using the word significant it might just be a standard that might be too high and that it would risk undermining the ability of consumers to take effective steps to protect themselves if there is a breach in security.

Mr. OLSON. And one more question, commissioner, a couple more. Does the commission see the concerns about the dangers of over-notification or, as my 14-year-old daughter and 11-year-old son would say, spam?

Ms. RAMIREZ. In my view, the greater danger is that consumers not be provided adequate notice to protect themselves against data breaches, so I don't believe that over-notification is a serious issue. I would be more concerned about not providing adequate protection if the standard were to be elevated.

Mr. OLSON. I am sure that we can agree that there is some balance there between over-notification and timely notification?

Ms. RAMIREZ. That is right. And I believe the reasonableness standard accommodates that.

Mr. OLSON. OK. Thanks for that. And one final question, why does the FTC feel so strongly about obtaining authority over nonprofits and universities for data security breaches?

Ms. RAMIREZ. The issue there is that, regardless of the nature of the particular entity, if the entity does have personal information about a consumer and there is a data breach, there is harm to the consumer regardless of whether that entity is either a nonprofit or a for-profit entity. So that distinction, in our view, would not provide adequate protection. So we are pleased to see that the draft bill does provide coverage for nonprofits.

Mr. OLSON. Yes, ma'am. Well, I am hearing some concerns from the nonprofit sector and the universities about this provision, and I would like to work with you forward and work with the chairman to resolve these concerns back home for the people I represent.

Ms. RAMIREZ. We would be pleased to do so.

Mr. OLSON. Thank you, ma'am. I yield back my time.

Mrs. BONO MACK. I thank the gentleman. And the chair recognizes Mr. Gonzalez for 5 minutes.

Mr. GONZALEZ. Thank you very much, Madam Chairwoman.

To my colleagues who have worked on this for the past few years, again, just that we continue down this road and haven't been successful yet, we passed things out of the House, and then we can't say that much about controlling anything that the Senate does, but it does mean that we will not be moving timely and aggressively.

To Mr. Stearns, thank you for his leadership. I still remember way back then, Cliff, when we used to say, don't collect it if you can't protect it. Remember we used to say that? And I think we are still saying that. And what has transpired since that time is that we haven't had the safeguards. We haven't had the review and the protections, of course. And we have just had—what have we had? We have had more breaches. I would like to think that had we had something in place, we would not have had the occurrences that have transpired recently.

Commissioner Ramirez, thank you very much for being here today. My questions are going to go to information brokers. And I do want to compare past efforts with the present effort, and hopefully, we can even improve what we have in the initial draft. H.R. 2221 had a lot as it related to information brokers. And I just want to get your opinion as to whether any new version of legislation should maybe also include some of these responsibilities that information brokers should be charged with. We had accuracy access and dispute resolution aspects or provisions when it came to brokers, but I am going to be a little more specific on some things that I believe at this early date the draft would not include, and I am going to ask whether you think it would be important that we would include these particular provisions: 2221 required information brokers to submit its security policies to the FTC, is that a good idea?

Ms. RAMIREZ. I think generally data security brokers need to be covered under any appropriate legislation, just as any other entity would be. If they collect information about a consumer, they ought to be covered.

Mr. GONZALEZ. 2221 permitted the FTC to conduct an audit or require each information broker to conduct an audit of its security practices, good provision?

Ms. RAMIREZ. Again, I think the data security measures that apply to other entities ought to apply equally to data brokers, because any entity that collects, gathers and uses personal information of consumers need to have appropriately protective data security measures.

Mr. GONZALEZ. Maybe even more so since that is your primary objective and activity, is it not, as opposed to someone else that, again, relative to their own commercial transaction may require certain information that is personal in nature and needs to be protected? But we are talking about information brokers. The very purpose of their existence is to do what?

Ms. RAMIREZ. I understand the point. All I am trying to say is that all entities that gather information that is personal to consumers create a potential risk of harm when there is a data breach.

So, from the commission's perspective, we don't want to draw distinctions. If an entity collects and uses consumer information there ought to be appropriate data security measures and absolutely they ought to apply to data brokers.

Mr. GONZALEZ. And that is the reason it was in 2221, and we would agree with you of course. The last two, because I have about a minute and a half, required the FTC to promulgate rules requiring information brokers to establish measures facilitating the investigation of breaches. Would that be important?

Ms. RAMIREZ. Yes.

Mr. GONZALEZ. And lastly, prohibit information brokers from pretexting, the practice of obtaining information through false representations?

Ms. RAMIREZ. Yes.

Mr. GONZALEZ. Thank you very much.

And I yield back Madam Chair.

Mrs. BONO MACK. I thank the gentleman.

And the chair recognizes Mr. Pompeo for 5 minutes.

Mr. POMPEO. Thank you, Madam Chairman.

Thank you for being here today, Ms. Ramirez. You talked about your concern for the exemption for publicly available information that you said that now with current technology, it has increased the value of that information. Can you give me an example of what you are thinking of?

Ms. RAMIREZ. I think there are a number of companies that gather information about consumers because it may aid, for instance, in connection with advertising and online behavioral advertising in particular. I know that the Wall Street Journal series has identified a number of companies that do this. It is an area that is of significant concern to the commission. And again, regardless of the fact that the information may be publicly available, given that it is now aggregated and it can be accessed technologically and much more easily, it raises significant data security concerns.

Mr. POMPEO. And what kind of information are you concerned about? Is it addresses? Tell me what it is that is publicly available that you are concerned about this aggregation of this information in the hands of these people you think are going to do harm.

Ms. RAMIREZ. It could be addresses. It could be names, family members that reside in a house. That combined with other information could potentially lead to security concerns.

Mr. POMPEO. Thank you.

I want to come back to something Congressman Stearns was speaking of. He was talking about the definition in the draft of legitimate business purposes. And if I understood your testimony correctly, you want to retain the authority, that you want the FTC to retain the authority to define that, that is to say we are going to apply a reasonableness standard, is that correct?

Ms. RAMIREZ. That is right.

Mr. POMPEO. Forgive me for my skepticism. I have been 16 years in business, and when the Federal Government says, don't worry, we will be reasonable, it causes alarm bells to go off in my head.

Ms. RAMIREZ. Perhaps it might help if I can articulate a concern. In many of these data breach cases, we find that information has been maintained for very lengthy periods of time when in fact the

company really had no reason to maintain that information. So that is why we, and I personally, believe that companies need to take greater care in ensuring that the consumer information that they maintain is needed. And if it is no longer needed, they should dispose of that information safely; otherwise, it just increases the potential for harm should there be a breach.

Mr. POMPEO. Suppose a company had some information, and they had no real current use for it, but they thought there might be value in that information 20 years from now. They might be able to sell their business, and somebody else might be able to use that information, but they couldn't touch today what exactly it is they thought the value of that was. But a legitimate business person, at least in that business owner's mind was, you know, I think there is value there. I worked to get that information. I obtained that information lawfully, and I now possess it, and I would just like to hang onto it because I think there may a good lawful use of that information sometime down the road. Would you consider that, after 10 or 20 years, would you consider that a legitimate business purpose in retaining that information?

Ms. RAMIREZ. I would be concerned that—there are many companies that do make that statement. My concern is that that is at odds with the desire to have adequate security. Because, again, the more that you keep information, the greater danger that it creates. So I am not going to sit here and say, it can only be after 5 years. I think there needs to be an appropriate assessment under particular facts and circumstances. But what we do advocate and I personally believe is that companies need to take a greater look at their practices, at their data security practices, to ensure that they minimize the possible risks of harm to consumers.

Mr. POMPEO. Right. I am not speaking to their practices in terms of securing that data. I am simply speaking to their desire to hold onto this thing that they view as their property, this thing that they have paid for and worked for and worked really hard to maintain, and they are engaged in the most capable security process you can imagine; they have not had a breach, and all they want to do is hold onto their property. But as I hear you, there is some risk that the FTC is going to come in and say, sorry, not legitimate?

Ms. RAMIREZ. No. Again, I think the standard to be applied is reasonableness. I think what the FTC and I personally believe is that companies simply need to take a stronger look and ask the question, do we really truly need this information, and not just simply use the concept of, oh, we may need it down the line without care to ask important questions about whether that information is entirely needed.

Mr. POMPEO. Great. Thank you.

Ms. RAMIREZ. And again, our focus is on information. I can just give you an example. I highlighted one case today, Ceridian, where Social Security numbers were being retained for a period when they were no longer needed in that particular instance. Again, there was no need to maintain those.

Mr. POMPEO. And when you say needed, you mean, in your mind, as opposed to in the company's mind?

Ms. RAMIREZ. The company no longer had reason to maintain those Social Security numbers, and unfortunately, there was a breach, and it created significant risk of harm to consumers.

Mr. POMPEO. Thank you. My time is expired.

Thank you, Madam Chairman.

Mrs. BONO MACK. I thank the gentleman.

The chair is pleased to realize the chairman emeritus of this committee, Mr. Dingell, for 5 minutes.

Mr. DINGELL. Thank you, Madam Chairman. Welcome, Commissioner Ramirez. I will be asking yes and no questions so I would appreciate your cooperation because time is short. Now, the draft legislation pending, our consideration exempts entities that must comply with the Gramm-Leach-Bliley Act or GLBA. The Federal Trade Commission's role to implement the data privacy requirements of GLBA is known as the safeguard rule, is that correct?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Now, Commissioner, does the safeguard rule require that covered entity, that a covered entity under the jurisdiction of the FTC notify a consumer of a data breach within a certain period of time, yes or no?

Ms. RAMIREZ. No, it does not.

Mr. DINGELL. Commissioner, so an entity regulated by FTC that is covered under GLBA, but not the draft bill, is under no statutory or regulatory obligation to notify consumers of a data breach within a time certain; is that correct?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Now, it would seem to me that we should consider removing the draft bill's GLBA exemption as well as to include H.R. 2221 60-day backstop notification in the interests of improving consumer protection. Now, the draft bill allows the Commission to modify the definition of the term "personal information" according to the Administrative Procedure Act, or APA, which I applied. I am worried, however, though, that the bill imposes vague conditions on the Commission to be satisfied before it could commence a rulemaking.

I fear that the effect would be that the Commission may never amend the definition of "personal information."

Now, Commissioner, has the Commission examined this matter and, if so, does the Commission share my opinion on the matter?

Ms. RAMIREZ. We do have concerns about the ability of the FTC to modify the definition of "personal information" as I articulated earlier in my testimony.

Mr. DINGELL. Now, I would request that the Commission submit its comments for the record. Would you do that for us, please, on this question?

Ms. RAMIREZ. Yes, of course.

Mr. DINGELL. Now, I understand the draft bill does not treat data brokers any different from other entities that collect and store personal information. This is a change from H.R. 2221, which by the way passed the House overwhelmingly, which describes additional requirements for data brokers.

The bill does not contain provisions that allow consumers to have reasonable access to information data brokers who collect information about them; is that correct?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Now, Commissioner, does the Commission believe that brokers should be subject to more stringent data security and breach notification requirements than other entities that collect and store personal information; yes or no?

Ms. RAMIREZ. In my view, yes.

Mr. DINGELL. Would you submit such amplification of that as you might deem appropriate?

Ms. RAMIREZ. Yes.

Mr. DINGELL. Now, Commissioner, does the Commission believe that consumers should have a statutory right to reasonable access of the personal information that data brokers collect about them; yes or no?

Ms. RAMIREZ. In my view, yes.

Mr. DINGELL. And I believe you would say that that is the only way you are going to assure that they will have that right to access; is that right?

Ms. RAMIREZ. In my view, yes.

Mr. DINGELL. Now, Madam Chairman, I appreciate your work on the bill so far, and I want to thank you for these hearings.

As my questions have indicated, I believe there are parts of the bill that can be improved. I stand by to work with you and am ready to assist you and the rest of our colleagues in order to report a bipartisan consensus bill that offers consumers the best protections possible. And I would observe, just quickly once more, the FTC has substantial experience in the protection of personal privacy from data collectors and things of that kind; is that not so, Madam Commissioner?

Ms. RAMIREZ. Yes.

Mr. DINGELL. So, Madam Chairman, I thank you for the courtesy and I yield back the balance of my time, which constitutes 37 seconds. Thank you.

Mrs. BONO MACK. I thank the gentleman very much and recognize Mr. Guthrie for 5 minutes.

Mr. GUTHRIE. Thank you very much. Thank you, Madam Commissioner, for being here.

I appreciate this and this is a serious issue that we have to address, and it looks like there is going to be significant work to do this in a way that is bipartisan. And I really didn't even think about this, and Mr. Pompeo said, but, you know, some of the things I learned when I was involved in the State legislature, involved in writing law and so forth, is that we have got to be as clear as we can because you see things—and just an example, you know, laws written 50, 60 years ago today are being used to, I think, doing interpretations by agencies that were never intended.

And so we just want to be careful that we are not just dealing with each other, and we know each other, and we know each other are thinking, but we have got to think what is going to happen as we go down the road.

And so in that, you know, I say, you have been there, and we had SEC here before and they said, well, we are trying to solve uncertainty. This may have to be decided in court if what we are doing is right. So when we look at words like "reasonable" and "significant risk," "reasonable risk," just kind of understanding what

we are thinking. And so I know we talk about reasonable risk in data security and significant risk.

And if you would kind of talk about the differences in those two and the cost of complying with this, I guess, for a business or in the level of security for consumers. We have got to decide, give this consumer the security they have, with the business having the knowledge or the certainty of what it is going to cost them to do, so they can plan and move forward.

So just the difference in reasonable and significant risk, in your mind, I guess.

Ms. RAMIREZ. In my mind, the concern that I had was that using the word "significant" would elevate the standards and the result would be that it would undermine protection to the consumer. The FTC has applied a reasonableness standard throughout its enforcement history in this arena, and it really does depend on the particular circumstances.

We would like to take into account, again, the nature of the information that might be at issue, the size of the company, the costs that might be involved. So I believe that taking a flexible approach allows us to fashion the right balance between the costs and burdens that may be imposed on business, as well as making sure that we have robust protection for consumers.

Now, I also want to highlight that the cases that the agency has brought in this arena have been—have related to very basic and fundamental failures in data security. These have not been close calls, so I hope that provides some assurance to those who may have concerns.

Mr. GUTHRIE. Yes. I am not an attorney, I did have one law school class, and the questions on tests aren't usually the obvious things, and that is where—usually there is some area that that is why it ends up in court; not that it is clear that somebody had data for 20 years, had Social Security numbers, had no need for them, and somebody breached them and took them.

As a matter of fact, at the expense of what a breach costs a company, I wouldn't want to hold on to that information more—if I didn't have a purpose or a need for it.

And I want to hit one thing and I will yield back. You talked earlier about the time for notification was too long, I guess in the draft you thought was too long. Did you say what you thought was reasonable for that, or what you suggest?

Ms. RAMIREZ. Our view is that notification ought to be provided as soon as practically feasible because, again, the circumstances may change. In certain situations it may be appropriate to have a short requirement of just a few days. In other situations, there may be a need for a company to take more time to write—to provide notifications.

So I think there ought to be an outer limit, and I have suggested that 60 days would be an outer limit but, again, that is an outer limit. Our view is the sooner, the better, because that allows consumers to take appropriate steps to mitigate any potential harm.

Mr. GUTHRIE. Oh, I agree with that. The difference is how we define—that is how we define it, so yes.

Ms. RAMIREZ. And, again, I think it is important to preserve some flexibility because it may differ depending on particular facts and circumstances.

Mr. GUTHRIE. Yes. I think there was one testimony in a previous hearing trying to figure out what happened, and they were trying to go through that. But you are right, because I mean, I would want to know as soon as practicable. Those were those words, you argued "practical" or "practicable," right?

Ms. RAMIREZ. Or "feasible."

Mr. GUTHRIE. But you are right. That is absolutely right. So I appreciate that look forward to working with the chairwoman and thank you for your courtesy.

Mrs. BONO MACK. I thank the gentleman. For not being a lawyer, you sure play one well on TV.

The chair is happy to recognize Ms. Schakowsky for 5 minutes.

Ms. SCHAKOWSKY. Thank you, Madam Chairman.

Let me just say that this committee has a history of working in a bipartisan basis, and the House did pass out H.R. 20—is it 21—whatever that brush bill was that I was a cosponsor of.

Ms. RAMIREZ. H.R. 2221.

Ms. SCHAKOWSKY. And, you know, we worked very closely together and, as Mr. Stearns says, it has been going on since 2005. I am so hopeful that we will be able to craft a bill. I feel confident that we will be able to craft a bill. In some respects this draft is even better, the quickness of certain notification. But we need to focus on, I think, where those differences are.

So let me just ask a couple of questions, Ms. Ramirez.

The Republican discussion draft includes language that I am concerned could have a narrowing effect that we don't totally understand. The draft narrows application of the bill's data security and notification requirements to persons engaged in interstate commerce with personal information, quote, "related to that commercial activity."

So let's take someone, a company like Amazon that is in the business of selling books. And in that process it generally collects your full name, address, credit card number and security code. But what if they also ask you for your Social Security number? I don't think they need that to sell a book. And if they did ask you for it, it probably wouldn't be to sell you that book. And what about other information that isn't at this time within the meaning of personal information like an IP address?

I know this is a fairly technical point so you may not have an answer right now, but to the extent you can, do you know how the FTC would interpret and implement this phrase, quote, "related to that commercial activity"?

Ms. RAMIREZ. I think we would interpret it to be coextensive with our jurisdiction over entities that engage in interstate commerce. I think it would be relatively broadly interpreted. Again, the precise scope of the definition is an area that we are happy to work with the committee to ensure that we assist in the committee coming up with a suitable definition that addresses the concerns that have been articulated today.

Ms. SCHAKOWSKY. Well, I am just worried that it is ambiguous language, and we may want to work with you and work with the committee to tighten that up.

Ms. RAMIREZ. And we would absolutely be pleased to work with you on that language.

Ms. SCHAKOWSKY. Great. Here we are, H.R. 2221 from the last Congress and the Republican discussion draft of the SAFE Data Act require notice to the FTC and consumers of an electronic data breach only if the covered person has determined that the breach, quote, "presents a reasonable risk of identity theft, fraud or other unlawful conduct."

I know that others have asked this, but I wonder if one more time, do you believe this trigger for notification, based on reasonable risk, et cetera, is appropriate?

Ms. RAMIREZ. I do. I think that the standard of reasonable risk gives it appropriate flexibility to accommodate both the need to protect consumers, as well as the need to take into account any burdens, excessive burdens on business.

Ms. SCHAKOWSKY. And it falls on the covered person to determine whether or not the trigger has been—for notification to the FTC and consumers—has been met. Do you believe it is appropriate for the covered person to make the ultimate determination about the risk posed to consumers from a data breach and whether notice to the FTC and consumers is required; and, if not, who should make that determination and how should they go about doing that?

Ms. RAMIREZ. That is a serious concern that we have. We believe that the FTC ought to be notified at the same time as other law enforcement agencies so that we can also examine the issue and determine if there ought to be notification that may differ from the determination that is made by the company.

Ms. SCHAKOWSKY. Thank you. And, finally, in the few seconds I have, H.R. 2221 would require notice to law enforcement, the FTC, and consumers in the event of a data breach involving electronic records. There is no requirement for notice in the event of a data breach involving paper records.

Do you believe the scope of the notification requirement should be expanded to include data breaches involving paper records?

Ms. RAMIREZ. I do. I believe that paper records can also pose serious concerns and risks to consumers.

Ms. SCHAKOWSKY. Thank you, and I yield back at zero.

Mrs. BONO MACK. I thank the gentlelady. The chair—I was going to give Christmas presents that equaled per seconds, like Christmas gifts would be valued by the size and the amount of time you give back.

The chair is happy to recognize Mr. Harper for 5 minutes.

Mr. HARPER. Thank you, Madam Chairman, and thank you, Commissioner, for being here and giving us your insight into this.

If I could just talk a little bit more about reasonable risk or significant risk, and you have indicated you support the reasonable risk standard.

How do you define that reasonable risk? What do you see that being?

Ms. RAMIREZ. I think if the information that is at issue is potentially going to be misused, can be misused to harm consumers, I think that there ought to be a presumption that there ought to be notification.

Again, I do—I do want to highlight that the agency has done significant work in this arena and our enforcement actions and consent orders that we have entered into, I think, can elaborate more fully on the situations that we have found where action was necessary. So, but again, I think there needs to be flexibility; I think reasonableness accomplishes that, and I would be concerned about changing that standard.

Mr. HARPER. So you said the Commission has done significant work versus reasonable work?

Ms. RAMIREZ. We have great experience in the area of data security.

Mr. HARPER. Right. So how would we vary with significant? If the standard was significant risk, how would you view that different than reasonable risk?

Ms. RAMIREZ. I think it is a flexible concept, and I don't have any magic words to articulate here today, but I think, in my mind, the key is how do we best protect consumers. And if that is the aim of the legislation, I believe that we ought to err in favor of protecting consumers, given that we know that the incidence of identity theft and data breach, by the way, is one significant cause, of, again, identity theft continues to be such a significant concern.

It is the most—we have received the most complaints relating to identity theft than any other complaint, and that has been in the last decade, so it remains a very significant concern.

Mr. HARPER. So "reasonable" would be in the eye of the beholder in some instances, is how we define this.

Ms. RAMIREZ. No. I believe that you can establish objective standards. The reasonableness of the concept that is, you know, well and defined in many different areas and used in many different areas of law, so I think it is one that can be employed in a way that I think would address concerns. I think it maintains appropriate flexibility and allows one to balance potentially competing interests.

Mr. HARPER. Yes. And I know as we go through the discussion draft and we look at it, there is going to be that discussion between reasonable and significant risk. You know, of course, as you know in the practice of law, some— you will have preponderance of the evidence, or, in a criminal case, beyond a reasonable doubt, but also there is clear and convincing.

So I think you are going to have that tug back and forth between reasonable and significant, wanting to protect the consumers but also looking at how the businesses will deal with this. So, you know, I appreciate your input on that.

As we look at the notification of when you believe FTC should be notified, you believe they should be notified at the same time as law enforcement. Is that what you have stated?

Ms. RAMIREZ. I do, yes.

Mr. HARPER. OK. And what period of time do you think is the optimum time for you to get that notification?

Ms. RAMIREZ. I think as soon as the breach takes place. I am now not remembering if the bill is specific on that point, but essentially at the very outset, when other law enforcement agencies are notified.

Mr. HARPER. When we look at that specific time limit, you know, these are certainly a great concern, as you have stated and as we know, data breach is something that everybody is concerned about and with this age that we have.

So tell me why you believe that the FTC should be notified prior to the consumers?

Ms. RAMIREZ. As a law enforcement agency, I think it is important that the FTC be provided prompt notification so that it can take appropriate action if necessary.

In addition, I think that waiting for the outcome of a particular company to engage in its own risk assessment risks a situation where a company may perhaps conclude that notification won't be necessary to consumers. The FTC may have a different view of it. It may provide an additional level of assurance as protection for consumers.

Mr. HARPER. Well, let me end with this quickly. Do you believe that this legislation, that it will address the current and evolving environment with respect to cloud computing?

Ms. RAMIREZ. I am sorry, could you repeat that?

Mr. HARPER. Do you think that this legislation appropriately addresses the current and evolving environment with respect to cloud computing?

Ms. RAMIREZ. I do. I think, again, cloud computing is, of course, the wave of the future. But the data security methods ought to apply to cloud computing, just as they do with other methods of storage.

Mr. HARPER. Thank you. With that, I yield back.

Mrs. BONO MACK. I thank the gentleman. The chair recognizes Dr. Cassidy for 5 minutes.

Mr. CASSIDY. Ms. Ramirez, the examples of health info which are not covered by HIPAA, can you give me those?

Ms. RAMIREZ. Let me give you an example from one of the matters that the FTC handled, the Eli Lilly matter, which involved the release of information about individuals who had used Prozac. HIPAA only covers particular entities such as hospitals, doctors' offices.

Mr. CASSIDY. So a noncovered entity, if you will.

Ms. RAMIREZ. It would be a noncovered entity; correct.

Mr. CASSIDY. Now, you—so this may answer my next question. It seems, as I am trying to understand this, that you in effect have two sets of data, one with unique identifiers and the other that is gained from publicly accessible information that you have a similar concern, even though it might not have a unique identifier; is that correct?

Ms. RAMIREZ. Well, it is not the issue of a unique identifier. Again, when it comes to public records, our concern is that once you compile information and you gather information that in the past might have been very difficult to collect, once it is collected at one place, that can then raise very serious concerns.

Mr. CASSIDY. So what are those concerns?

Ms. RAMIREZ. When you have data aggregators that are gathering information about——

Mr. CASSIDY. Well, I understand what a data aggregator is, I understand that. They get all the data about mortgages being sold in Washington, D.C.

Ms. RAMIREZ. One example could be that they may have information that might—can be given to a payday lender, for instance, because they have information that may reveal—have indications about income level. That information can then be used by a payday lender or someone who aims to engage in some type of fraudulent activity.

Mr. CASSIDY. Now, a payday lender is not inherently fraudulent?

Ms. RAMIREZ. No, no, no, no, no. But my point is it can be used by persons who may want—seek to misuse that information, so it is very important that that information——

Mr. CASSIDY. But that is true of all information in a free society; correct? I am nervous about limiting access to publicly available information, and I don't necessarily disagree with you, but it always seems like we should have a bias towards openness, knowing that those—so why should we not have this bias towards openness if it is not being used by a fraudulent entity and if it is publicly available otherwise?

Ms. RAMIREZ. The key is to ensure that appropriate measures are taken to protect the information that has been aggregated. You then—you now have an ability with these data aggregators who have gathered just a treasure trove of information that, again, previously may not have been easily accessible.

Mr. CASSIDY. You keep saying that, and I understand that. I understand that issue. What I don't know is what danger you see with that. And I am asking openly.

Ms. RAMIREZ. So the danger can be that it can be misused for a number of reasons.

Mr. CASSIDY. But I guess all information could be misused. All information can be misused. And so I am just trying to understand.

Ms. RAMIREZ. So the fundamental point is that that information needs to be protected; and if that information, if there has been a breach, the consumer ought to be notified. And in the case of data brokers, I believe that there ought to be some additional requirements where a consumer may have access to that——

Mr. CASSIDY. Just so I understand better, because clearly I am struggling, can you give me a specific example of—and just so I can understand—again, I am not challenging, I am trying to understand—a specific example of where a data aggregator had data that was breached that did not include a Social, did not include a credit card number or a security code, it was just like, you know, Bill Cassidy, the Congressman from Baton Rouge, and he has got three kids and et cetera, et cetera. Are you with me?

Ms. RAMIREZ. Let me give you one example. Information relating to income, for instance, is information that might be gathered or somehow ascertained through the access of publicly available information.

Mr. CASSIDY. Now I am told, when I suddenly saw all these catalogs that I was getting back from people who send catalogs, that they looked at my census track and said, oh, he is in a pretty good

census track, and so therefore I started getting an incredible number of catalogs. Now, are we going to restrict the ability of someone to know what census track I live in?

Ms. RAMIREZ. No, but I think you can provide access rights so that if, for instance—again let me go back to——

Mr. CASSIDY. Now the access rights is a separate issue. The access rights, I gather from Mr. Dingell's thoughts, and it actually seems—I can see some use in that.

But, again, I am wondering, what is the inherent damage——

Ms. RAMIREZ. We would not be restricting the ability to gather the information that was publicly available. We would simply want there to be adequate security measures to protect the information, and we would want there to be notification to the consumer in appropriate circumstances. And in light of potential misuse of information, additional requirements such as access may be one way of addressing. But I am not advocating that there be a limitation on the ability——

Mr. CASSIDY. As the risk of losing my Christmas presents, I will say, though, that it almost seems that if you have one with credit card numbers and Socials and medical, you know, military identification numbers, that clearly should be in its own silo.

The other seems—the other seems, I am not sure—and I am sure there is going to be an expense in terms of being in the silo. The other seems to me to be inherently less, I don't know, onerous as regards the protective measures taken, because it doesn't have the same import if somebody knows I have got three kids and live in the census track as opposed to knowing my Social.

Ms. RAMIREZ. My apologies if I haven't been able to fully articulate the potential risks that we see, and my staff is very happy to work with you to provide some additional information if I have not been able to answer your question adequately.

Mr. CASSIDY. If you will do that. And, again, I would just understand. If you all send it to me, I would appreciate it.

Thank you. I yield back.

Mrs. BONO MACK I thank the gentleman. I recognize Mr. Rush for 5 minutes.

Mr. RUSH. I want to thank you, Madam Chairman. We have known for several Congresses now that mass MEGA data breaches could and will occur. And we have had the vision to introduce legislation to make these breaches more difficult to perpetuate and that would make consumers as close to whole as possible when they piece back together their personal lives and identities.

The DATA Accountability and Trust Act that I reintroduced in May, along with Congressman Barton and Congresswoman Schakowsky, is essentially the same bill that was passed out of this committee in December of 2009, in the 111th Congress, as H.R. 2221. That bill passed out of the House on suspension and was then referred to the Senate Commerce Committee.

When I became chair of this subcommittee in the 110th Congress, I introduced H.R. 958, which has since been shaped to keep up with online and network technologies and emerging formats for storing consumer data. These technologies and formats improve consumers' lives and make new and exciting business efforts and revenue models viable. But it has been important in our approach

to remain technologically neutral, so that we don't pick winners and losers, and also cognizant—and remain cognizant of the unique natures of the business models and realities involving what the bill defines as "service providers," "information brokers," and "fraud databases."

Madam Commissioner, I only have a few minutes and so I am going to ask you a few questions, and I intend to ask each panel these questions. So if I could get a yes or no answer, that would certainly help me. And if I don't get to ask the questions, I have some that I will refer to you in writing for the record.

Should commercial entities that do business in interstate commerce be required under Federal law to protect individuals' personal information by securing it and protecting it from improper access?

Ms. RAMIREZ. Yes.

Mr. RUSH. And when these entities contract with a third party to maintain that personal data, should they be further required to establish and implement information, security policies, and procedures?

Ms. RAMIREZ. Yes.

Mr. RUSH. Should the FTC be authorized to prescribe what those policies and procedures ought to be?

Ms. RAMIREZ. Yes.

Mr. RUSH. Should personal information be defined to include an individual's first name or initial and last name, or address, or phone number, in combination with any—with any one or more of the following. An individual's Social Security number?

Ms. RAMIREZ. I believe that that would be too narrow a definition.

Mr. RUSH. I have got a number of them, yes or no. Yes or no.

Ms. RAMIREZ. No.

Mr. RUSH. A driver's license number?

Ms. RAMIREZ. No.

Mr. RUSH. A passport number, military number, or similar identification number issued on a government document for verifying identity?

Ms. RAMIREZ. No.

Mr. RUSH. A financial account number?

Ms. RAMIREZ. No.

Mr. RUSH. A credit card number?

Ms. RAMIREZ. No.

Mr. RUSH. A debit card number?

Ms. RAMIREZ. No.

Mr. RUSH. Or any security, access code, or password needed to access the account?

Ms. RAMIREZ. No.

Mr. RUSH. Should information brokers be required to submit their data security policies to the FCC?

Ms. RAMIREZ. Yes.

Mr. RUSH. Should information brokers be required to establish procedures that consumers may follow to review and, if necessary, dispute the accuracy of their personal data?

Ms. RAMIREZ. In my view, yes.

Mr. RUSH. Thank you very much. You have been very kind and helpful.

With that, Madam Chair, I yield back the balance of my time.

Mrs. BONO MACK. The chair recognizes Mrs. Blackburn for 5 minutes.

Mrs. BLACKBURN. Thank you, Madam Chair, and thank you for being here with us today.

I want to stay with this personally identified information, because I think that gets to kind of the crux of the matter when you talk to our constituents and you look at how they have reacted to what has transpired with the Sony breach and the amount of time that was required to inform people there. You can go back as far as the TJX breach and the amount of time and the inconvenience that was caused to individuals there.

So I think that what we have to do is that our goal should be to define this legislation in a way that is very clear and very meaningful to our constituents and to policymakers. And I know Mr. Stearns talked about FTC control and authority, and some people believe that we should not give the FTC the control to make the policy. Specifically, the FTC with the rulemaking process and having the ability to set what is personally identified information is a very powerful tool, and there are many that think we should define that in law and not give it to the FTC.

So I want to stay with this. I want you to define for me, just go down the tick list of—as making rules, what you would put sequence, what would be personally identified information, how you would sequence that in the rulemaking authority.

Ms. RAMIREZ. I think the touchstone here is information that can be uniquely tied to an individual. I am afraid that I just can't rattle off a list here, but my staff is very happy to work with you to articulate in more specific terms. But, again, the key would be information that can then be used to identify someone. And I believe it would be broader than the definition that is currently used in the draft bill.

Mrs. BLACKBURN. OK. What I would like for you all to do, then, is to submit that to us in writing, because I think this is an area where we are going to need to focus, put some attention on what this is, who owns that online presence; is it becoming more important to our constituents? And we hear from them daily on the privacy issue, on the data searching, the data selling, all of these issues that are becoming intertwined, even with the piracy issue and the intertwining that is there.

So to say a unique tie may be a simple, concise answer to give, but it does not provide the depth that we are going to need and have as we go through this. So I would ask you to do that.

OK. The chair talked about declaring war on identity theft and online fraud, and I think she is exactly right on this because—and I agree with her on this, and our constituents look at this as a virtual marketplace that is out there. And they look at the relationship they have had with brick-and-mortar retails and entities and then with click-and-mortar businesses and also virtuals. So let's talk about people who have become the victim of identity theft. What services do you think should be made available to them? Peo-

ple realize a free credit report doesn't cut it. Credit monitoring doesn't cut it.

So tell me what you think for those that have been harmed by identity theft. What services should be available for them?

Ms. RAMIREZ. I do think that credit monitoring is an important aspect of the protection, but I also think it is incumbent—what the consumer will need to do is to be very vigilant, monitoring all of their financial accounts, monitoring their billing statements, and if they see anything, so that——

Mrs. BLACKBURN. So the personal responsibility aspect.

Ms. RAMIREZ. That is an element of it. And we provide guidance to consumers about what they ought to do and the steps that they ought to take.

Mrs. BLACKBURN. So you see the FTC's role more as providing guidance on that.

Ms. RAMIREZ. In terms of—consumer education is a significant piece of what the FTC does, and we do provide significant information to consumers, helping them take steps if their identity has been stolen or there is a risk of that, what steps they can take to protect themselves.

Mrs. BLACKBURN. OK. Let me ask you one other thing. The bill that we are considering, should it apply to government systems?

Ms. RAMIREZ. The bill should apply to commercial activity. That is the jurisdiction that the FTC has to commercial entities, so that is the scope of our jurisdiction.

Mrs. BLACKBURN. And you don't think we should apply it to government entities?

Ms. RAMIREZ. It is an area that is outside the scope of what the FTC does.

Mrs. BLACKBURN. I respect that answer. Thank you very much. I yield back.

Mrs. BONO MACK. I thank the gentlelady very much.

With that, we have concluded the first panel. We want to thank our witness very much for her in-depth and very thoughtful answers today.

I will say to the audience, we are going to take a 5-minute break while we reseat the second panel, but to remind people that there is an overflow room in 2123 for anybody who would prefer to sit rather than stand.

So, again, Commissioner Ramirez, thank you very much for your time today.

Ms. RAMIREZ. Thank you.

Mrs. BONO MACK. See you all in 5 minutes.

[Recess.]

Mrs. BONO MACK. All right. If the subcommittee could come to order once again. If the gentleman in the corners could please take your seats.

On our second panel we have four witnesses who are deeply engaged on the issue of cybersecurity.

Testifying are Jason Goldman, Counsel, Telecommunications & E–Commerce, U.S. Chamber of Commerce; Robert Holleyman, President and CEO of the Business Software Alliance; Stuart Pratt, President and CEO of the Consumer Data Industry Association;

and Marc Rotenberg, Executive Director for the Electronic Privacy Information Center.

Good afternoon, gentlemen. Thank you all for coming. You will each be recognized for 5 minutes. To help you keep track of the time there is a time clock in front of you, and green, red, yellow, you know what they mean. Yellow means 1 minute to get to the conclusion of your testimony.

STATEMENTS OF JASON D. GOLDMAN, COUNSEL, TELECOMMUNICATIONS & E-COMMERCE, U.S. CHAMBER OF COMMERCE; ROBERT W. HOLLEYMAN, II, PRESIDENT AND CEO, BUSINESS SOFTWARE ALLIANCE; STUART K. PRATT, PRESIDENT AND CEO, CONSUMER DATA INDUSTRY ASSOCIATION; AND MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mrs. BONO MACK. So at this point in time we are going to recognize Mr. Goldman for 5 minutes, and please remember to turn your microphone on and bring it close to your mouth.

STATEMENT OF JASON D. GOLDMAN

Mr. GOLDMAN. Good afternoon, Chairwoman Bono Mack, Ranking Member Butterfield, and other distinguished members of the subcommittee. I am Jason Goldman, Telecommunications & E-Commerce Counsel of the U.S. Chamber of Commerce, the world's largest federation, business federation, representing the interests of more than 3 million businesses and organizations of every size, sector, and region.

On behalf of the Chamber and its members, I thank you for the opportunity to testify here today regarding the discussion draft of the SAFE Data Act.

We live in an information economy. Today, Chamber members of all shapes and sizes communicate with employees, existing consumers, potential consumers, and business partners around the world. They use data to spur sales and job growth, enhance productivity, enable cost savings and improve efficiency.

Global and U.S. data usage are skyrocketing. In today's tough economy, businesses depend more than ever on having beneficial and trusted relationships with their customers. Therefore, there is no question that protecting sensitive customer information should be a priority for all businesses that collect and store this data, and the customers deserve to be promptly notified if a security breach has put them at risk of identity theft, fraud, or other harm.

The Chamber supports the enactment of meaningful Federal data security legislation that would implement national data security standards to protect against the unauthorized access to sensitive personal information about businesses' customers, and breach notification requirements to notify customers when a significant risk to them may result from a security breach. At the same time, the Chamber urges policymakers to ensure that any legislation in this area does not hinder innovation and beneficial uses of the data.

The Chamber appreciates the willingness of the subcommittee to work with us in legislation aimed at accomplishing this goal. The Chamber only recently got this text of the SAFE Data Act, so our

comments are based on our initial read and may change as we continue to vet the bill through our membership.

The United States has a national economy. And almost every State has enacted various data security and breach notification provisions, many of which differ from one another in material ways. This patchwork of State laws not only makes compliance difficult for businesses, but it can also create confusion for customers who receive notices from many sources.

The Chamber supports the preemption of State information security and related liability laws to create a national uniform standard that will create regulatory certainty and minimize compliance costs for businesses that operate in multiple States.

The Chamber has long advocated for a notice requirement that avoids the dangers of over-notification. As was discussed in the previous panel, the Chamber worries that if needlessly alarmed, customers may take actions that are not warranted and are a waste of their time.

Alternatively, more worrisome, customers that are flooded by these notices may be falsely lulled into inactivity and not take proper action when the risk is justified.

Therefore, the Chamber is pleased that the draft bill recognizes that the notification should be based on risk of harm, not just on the mere fact that data breach occurred.

The Chamber agrees that notification of breach is not necessary where the data has been rendered unusable, unreadable, orindecipherable by different methods such as encryption, redaction, or access controls.

The Chamber also recommends the inclusion of a threshold number of individuals requiring notification that would trigger notification to the FTC.

The Chamber agrees that consumers should be notified in a timely manner after the occurrence of a reportable breach. However, given the complexities of dealing with a data breach, the Chamber recommends that the draft be modified to allow companies a reasonable amount of time to notify consumers, rather than a specific time frame.

Furthermore, to catch cybercrooks and other criminals, as well as to ensure the safety of our Nation, the Chamber supports the revisions in the draft bill permitting delay of notification for law enforcement or national security purposes. Along with that, the Chamber recommends inclusion of language in the bill that identifies which specific agencies would trigger that exception or would have been able to enact that exemption.

Regarding liability, the Chamber is concerned about the application of a daily fine as it relates to the bill's security requirements. If any entity is found liable for violating the data minimization requirement, is every day the entity maintains records that should have been destroyed throughout all of their data bases a multiplier penalty?

The Chamber appreciates the revisions on the data broker provisions that were discussed in the panel earlier.

On enforcement, the Chamber is concerned about enabling State attorneys general to impose 50 different enforcement regimes that will undermine the uniformity of this act and make compliance ex-

tremely difficult. At the very least, the draft bill should curtail the ability of State attorneys general to utilize private outside contingency attorneys to enforce this act or to litigate claims on behalf of their constituents.

Also the Chamber appreciates the tech-neutral provision in the act that says the FTC should implement in a tech-neutral manner. And, last, the Chamber does appreciate the inclusion of a prohibition of the no private right of action.

With that, thank you, and I am happy to answer any questions.

Mrs. BONO MACK. Thank you, Mr. Goldman.

[The prepared statement of Mr. Goldman follows:]

Statement of the U.S. Chamber of Commerce

ON: **H.R. ___, A DISCUSSION DRAFT TO REQUIRE GREATER PROTECTION FOR SENSITIVE CONSUMER DATA AND TIMELY NOTIFICATION IN CASE OF BREACH**

TO: **UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON ENERGY AND COMMERCE, SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE**

BY: **JASON D. GOLDMAN**
COUNSEL, TELECOMMUNICATIONS & E-COMMERCE
U.S. CHAMBER OF COMMERCE

DATE: **JUNE 15, 2011**

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

More than 96 percent of the Chamber's members are small businesses with 100 or fewer employees, 70 percent of which have 10 or fewer employees. Yet, virtually all of the nation's largest companies are also active members. We are particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large.

Besides representing a cross-section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business – manufacturing, retailing, services, construction, wholesaling, and finance – is represented. Also, the Chamber has substantial membership in all 50 states.

The Chamber's international reach is substantial as well. It believes that global interdependence provides an opportunity, not a threat. In addition to the U.S. Chamber of Commerce's 113 American Chambers of Commerce abroad, an increasing number of members are engaged in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on national issues are developed by a cross-section of Chamber members serving on committees, subcommittees, and task forces. More than 1,000 business people participate in this process.

Hearing on H.R. ___, A Discussion Draft to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach

Testimony of Jason D. Goldman
Counsel, Telecommunications & E-Commerce
U.S. Chamber of Commerce

June 15, 2011

Good morning, Chairwoman Bono Mack, Vice Chairwoman Blackburn, Ranking Member Butterfield, and other distinguished members of the Subcommittee on Commerce, Manufacturing and Trade. I am Jason Goldman, Telecommunications & E-Commerce Counsel at the U.S. Chamber of Commerce, the world's largest business federation, representing the interests of more than three million businesses and organizations of every size, sector, and region. On behalf of the Chamber and its members, I thank you for the opportunity to testify here today regarding the discussion draft of the "Secure and Fortify Electronic Data Act" (the "SAFE Data Act").

I. Information Economy

We live in an information economy. Today, Chamber members of all shapes and sizes communicate with employees, existing customers, potential customers, and business partners around the world. They use data to spur sales and job growth, enhance productivity, enable cost-savings, and improve efficiency. For example, the beneficial use of U.S. health care data could result in $300 billion in value to health care consumers each year, including reducing national expenditures in this area by $200 billion or 8 percent.[1] The power of data also could help retailers boost their profit margins by as much as 60 percent.[2]

Global and U.S. data usage will continue to skyrocket. The "gigabyte equivalent of all movies ever made will cross global IP networks every five minutes" by 2015, according to Cisco.[3] U.S. mobile data traffic is expected to increase by 21 times from 2010 to 2015.[4] As consumers embrace tablets, smart appliances, and other wireless broadband-enabled devices,

---

[1] McKinsey Global Institute, *Big Data – The Next Frontier for Innovation, Competition, and Productivity*, p. 2, May 2011, *available at*: http://www.mckinsey.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf.

[2] *Id.*

[3] White Paper, *Cisco Visual Networking Index: Forecast and Methodology, 2010–2015*, Cisco Systems, Inc., June 1, 2011, *available at:* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

[4] Press Release, *Cisco Visual Networking Index Forecast Projects 26-Fold Growth in Global Mobile Data Traffic From 2010 to 2015*, Cisco Systems, Inc., Feb. 1, 2011, *available at:* http://newsroom.cisco.com/mobile/dlls/2011/prod_013111.html. (*"Cisco Visual Networking Index Forecast Global Mobile Data Forecast").*

mobile network traffic will soar. Mobile-connected tablets will generate as much traffic in 2015 as the entire global mobile network in 2010, growing over 205-fold over that same time period.[5]

In today's tough economy, businesses depend more than ever on having beneficial and trusted relationships with their customers. Therefore, there is no question that protecting sensitive consumer information should be a priority for all businesses that collect and store this data, and that consumers deserve to be promptly notified if a security breach has put them at risk of identity theft, fraud, or other harm.

II. *SAFE Data Act*

The Chamber supports the enactment of meaningful federal data security legislation that would implement national data security standards to protect against the unauthorized access to sensitive personal information about businesses' customers and breach notification requirements to notify customers when a significant risk to them may result from a data security breach. At the same time, the Chamber urges policymakers to ensure that any legislation in this area does not hinder innovation or the beneficial uses of data.

The Chamber appreciates the willingness of the Subcommittee to work with us on legislation aimed at accomplishing this goal and believes that this bill contains improvements in several areas that raised concern in similar legislation that was considered by the full Committee and the full House in the 111th Congress.

The Chamber only recently received the text of the SAFE Data Act, so the comments below are based on our initial read of the bill and may change as we further analyze the language and vet the bill through our membership.

a. Federal Preemption

The United States has a national economy, and almost every state has enacted various data security and breach notification provisions, many of which differ from one another in material ways.[6] This patchwork of state laws not only makes compliance difficult for businesses, but can also create confusion for consumers who receive notices from many sources. The Chamber supports the preemption of state information security and related liability laws to create a national uniform standard that would create regulatory certainty and minimize compliance costs for businesses that operate in multiple states.

---

[5] *Cisco Visual Networking Index Forecast.*

[6] *State Security Breach Notification Laws*, National Conference of State Legislatures, Oct. 12, 2010, *available at*: http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx. ("Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.")

b. Breach Notice Trigger

The Chamber has long advocated for a notice requirement that avoids the dangers of over-notification. If needlessly alarmed, consumers may take actions that are not warranted and waste their time. Alternatively and more worrisome, consumers that are flooded by notices may be falsely lulled into inactivity and not take proper action when a true risk is identified. Therefore, the Chamber is pleased that the draft bill recognizes that notification should be based on risk of harm, not just on the mere fact a data breach has occurred. There is a tremendous difference between a breach that creates the possibility of identity theft and a breach where no or little risk is created. Additionally, the Chamber recommends changing the standard from "reasonable risk" to "significant risk."

Moreover, Congress should place restrictions on the Federal Trade Commission's (Commission) ability to define "harm" when examining risk. It is of course incredibly important for the government to fulfill its traditional role of protecting consumers from financial theft, physical injury, and other tangible forms of harm. However, any move to broaden the definition of "harm" should be carefully considered.

The Chamber agrees that notification of a breach is not necessary where the data has been rendered unusable, unreadable, or indecipherable by a commonly-accepted, effective industry standard or industry practice, such as encryption, redaction, or access controls. The Chamber encourages a technology-neutral approach to this provision that keeps the Commission, which may not have the requisite expertise, from having the responsibility of determining the adequacies of these technologies.

The Chamber recommends the inclusion of a threshold number of individuals requiring notification that would also trigger notification to the Commission. One option is 5000, which is the draft bill's threshold for notification to credit agencies. Another option is 500, the threshold for notice to the Department of Health and Human Services under the Health Information Technology for Economic and Clinical Health ("HITECH") Act. If neither of these provisions is adopted, then the draft bill should direct the Commission to issue guidance about what criteria the agency will use to determine which breaches are listed on the agency's Web site. Without such guidance, the Commission could potentially post all breaches, no matter the severity.

c. Breach Notification Timing

The Chamber agrees that consumers should be notified in a timely manner after the occurrence of a reportable data breach. However, given the complexities of dealing with a data breach, the Chamber recommends that the draft bill be modified to allow companies a "reasonable" amount of time to notify consumers, rather than a specific timeframe (i.e., 48 hours).

Adopting a "reasonable" timeframe would help to ensure that consumers are notified when there is a true risk and avoids over-notification that may lead to consumer overreaction and inconvenience (e.g., needlessly cancelling a credit card). Also, it is important to note that each layer of requirements that must be completed, included, or offered (e.g., arranging for credit

report monitoring or issuing replacement credit cards) as part of the breach notification potentially adds to the time that it takes to prepare and issue the notification.

To help catch cybercrooks and other criminals as well as to ensure the safety of our nation, the Chamber supports the provisions in the draft bill permitting delay of notification for law enforcement or national security purposes. It is proper to delay notification to avoid impeding civil or criminal investigations. Additionally, if it is determined that notification would harm national or homeland security, delay is certainly appropriate. Additionally, the Chamber recommends the inclusion of language to clarify which state or federal agencies (such as the Department of Homeland Security) that a company can reasonably rely upon for this exemption.

d. *Liability*

The Chamber is concerned about the application of a daily fine as it relates to the draft bill's security requirements. For example, if an entity is found liable for violating the data minimization requirement, is every day that the entity maintains records that should have been destroyed throughout all of their databases a multiplier penalty? Companies could potentially be in permanent violation.

e. *Data Minimization*

The determination of what information to collect is different for each company and business plan. The Chamber is concerned that a data minimization requirement could lead to regulatory uncertainty. Rather than risk liability, companies may self-censor themselves. By taking such action, these companies may fail to realize the full, legitimate benefits of their data. Innovation and economic activity could suffer. Thus, the Chamber recommends that the draft bill should encourage data minimization as a goal, not a requirement.

f. *Information Brokers*

Information brokers provide information that is used in many beneficial ways in our economy and by our society, including: fair and efficient consumer credit allocation; local and national background employment screenings and national security clearances; fraud prevention in the private-sector and in government; the collection of child support payments; and assistance to law enforcement, private agencies, public and private-sector investigators on matters ranging from locating missing and exploited children to preventing money laundering and terrorist financing.

The Chamber is pleased that the draft does not include provisions contained in last year's bill (H.R. 2221) that could unintentionally reduce consumer protection by endangering the establishment and use of databases that are designed to protect consumers, such as those intended to stop fraud and identity theft.

g. Enforcement

The Chamber is concerned that enabling state attorneys general to impose 50 different enforcement regimes will undermine the uniformity of this Act, and will make compliance exceedingly difficult. Alternatively, this provision should be transparent and consistent with existing law (i.e., the Fair Credit Reporting Act). At the very least, the draft bill should curtail the ability of state attorneys general to utilize private outside contingency fee lawyers to enforce this Act or to litigate claims on behalf of their constituents.

h. Technology Neutral

The Chamber urges policymakers to ensure that federal laws and regulations are technology-neutral. The government should not be in the position of picking technology winners and losers. The marketplace, not government fiat, is the best way to ensure technological innovation and consumer choice.

Therefore, the Chamber is pleased that the draft bill directs the Commission to promulgate rules under this Act in a technology-neutral manner. Specifically, the draft bill prohibits the Commission from requiring the deployment or use of any specific products or technologies, including any specific computer software or hardware.

i. No Private Right of Action

Though the Chamber would prefer the inclusion of explicit language prohibiting private rights of action, the Chamber supports Section 6(b)(1) of the draft bill. Allowing private lawsuits would only serve to increase the likelihood that elements of the plaintiffs' class action trial bar will use this legislation as a way to increase class action litigation with little benefit being given to the general public. Additionally, a perverse incentive not to notify consumers of a data breach could be created if entities covered under the draft bill become worried about opening themselves to potential law suits.

j. Definitions

For the definition of "service provider," the Chamber recommends adopting language that more closely tracks the definition of telecommunications in the Telecommunications Act.[7] One option may be to use the language in H.R. 1707, the "Data Accountability and Trust Act," which defines "service provider" as:

> [A]n entity that provides to a user transmission, routing, intermediate and transient storage, or connections to its system or network, for electronic communications, between or among points specified by such user of material of the user's choosing, without modification to the content of the material as sent or received. Any such entity shall be treated as a service provider under this Act only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage or connections.

[7] 47 U.S.C. § 153(50).

III. Conclusion

Once again, the Chamber greatly appreciates the opportunity to testify today. The Chamber stands ready to work with you on these and other issues. Thank you very much.

Mrs. BONO MACK. Mr. Holleyman, you are recognized for 5 minutes.

STATEMENT OF ROBERT W. HOLLEYMAN, II

Mr. HOLLEYMAN. Chairwoman Bono Mack, Mr. Butterfield, members of the committee, Business Software Alliance strongly supports the enactment of a national data security and data breach notification law. We believe that that is important to build trust and confidence in the digital economy.

This is now the fourth Congress to consider data breach legislation, and we are grateful for the opportunity that we have had to work with the members of this committee to advance a bill.

The time to act is now. The need is clear, as are the solutions. BSA endorses the key elements of the SAFE Data Act that are before us today. We support requiring organizations that hold sensitive personal information to implement reasonable security procedures. And the draft bill takes into account an organization's size, the scope of its activities, and the costs involved.

We support creating incentives to adopt strong security measures. The draft bill will promote the use of technologies such as encryption, which render data unusable, unreadable, or indecipherable to thieves if they manage to steal it. We support an approach that avoids unnecessarily alarming or confusing consumers, and the draft bill accomplishes that by only requiring notification when there is a risk of identity theft, fraud, or unlawful activity.

Finally, we support the bill's establishment of a uniform, national framework with Federal enforcement preempting today's patchwork of State laws.

We hear about new data breaches almost daily. One group, the Privacy Rights Clearinghouse, has recorded more than 2,500 of them since 2005, involving more than 530 million individual records. In many cases these records include data that are useful to identify individuals and then exploited by thieves, such as Social Security, credit card, or driver's license numbers.

Surveys indicate that these breaches are causing consumers to question the security of online transactions, and that is especially troubling, because we are in the middle of an exciting new wave of innovation with the emergence of cloud computing. Cloud computing offers tremendous new opportunities for economic growth and efficiency. It allows businesses and organizations to reinvent their back office operations and will give users access to their data and services from any device, whether they are at home, at the office, or on the road.

We cannot allow breaches to erode confidence in the cloud environment or the Internet economy, and for years BSA members have been working hard to protect data from cybercriminals. BSA members are leaders in providing new security solutions and themselves invest in reducing vulnerabilities and protecting the integrity of their technology.

BSA members are developing cutting-edge security solutions that are employed by businesses and consumers to defend against the evolving and the very real threats. And BSA has led the fight against the use of illegal software, not only because it drains revenues from American companies, but also because pirated software

commonly includes malicious computer code that hackers and other criminals use to steal data. Importantly, BSA members are at the forefront of the cloud revolution, which creates new opportunities to better store data behind strong security walls.

As this committee understands, Congress also has a responsibility. In the absence of a national law, States have enacted their own data breach notification requirements. Unfortunately, this has resulted in inconsistency that is unwieldy for business and confusing for consumers. We need a uniform national framework that better protects consumers and also, as this bill does, promotes effective security measures.

I testified before this committee 2 years ago about the need for a national data breach law. Since then, another 250 million sensitive records have been breached.

Madam Chairman, I commend you and your colleagues for drafting this bill. I urge Congress to pass a Federal data breach law this year. And the BSA and I look forward to working with you and members of this committee to make that a reality.

Mrs. BONO MACK. Thank you very much, Mr. Holleyman.

[The prepared statement of Mr. Holleyman follows:]

Subcommittee on Commerce, Manufacturing and Trade
June 15, 2011 Hearing on Data Security and Breach Notification Legislation
Summary of Testimony of Robert W. Holleyman II (BSA)

BSA believes Congress must pass this year federal legislation that requires organizations to secure the sensitive personal information they hold, and to notify individuals when that security has been breached, can effectively enhance consumers' trust. BSA recommends that such legislation pursue the following objectives, which we are pleased to see reflected in the draft bill.

Establish a uniform national standard that preempts state laws—Forty-six States, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands had enacted data breach notification laws. This patchwork has created a compliance nightmare for businesses, as well as confusion for consumers who receive notices from a multiplicity of sources. We are heartened by the draft bill's inclusion in section 6 of language pre-empting state laws, and suggest that the scope of preemption be clarified to cover notification to government agencies as well as private parties.

Prevent excessive notification—Some breaches create great risks of harm to consumers, while others create little to no risk. Currently, most state data breach laws require notification even when no risk exists. Over notification is likely to confuse consumers, who will then fail to take appropriate action when they are truly at risk. We believe notification should be required only in those instances where an unauthorized disclosure presents a significant risk of material harm. We are pleased that section 3(f) of the draft bill takes a risk-based approach to breach notification. We recommend that the threshold be "*significant risk,*" to ensure that only genuine risk is notified.

Exclude data that has been rendered unusable, unreadable, or indecipherable—Data not be subject to breach notification if it has been rendered unusable, unreadable, or indecipherable through practices or methods, such as encryption, redaction, or access controls, which are widely-accepted as effective industry practices or industry standards. The draft bill's section 6(f)(2) provides a market-based incentive for the adoption of strong data security measures. We recommend however that this provision be made technology. As drafted, we are concerned that it may tilt the playing field by setting up a two-tiered approach: while encryption is explicitly listed in the draft bill, other methods would require the sanction of an FTC rulemaking.

Require the use of data security safeguards—in addition to requiring breach notification Congress should prevent breaches from happening in the first place, by requiring organizations that hold sensitive personal information to establish and implement data security policies and procedures. We support the fact that the draft bill does this in section 2. It is also important to avoid over-regulating data custody. While we support the draft bill's requirement that organizations protect the consumer data that they hold, we are concerned that the grant of authority to the FTC, in section 2(a)(1), to develop a body of regulations governing such corporate policies and procedures will in effect make the activity of data custody a regulated activity. The specificity of the data security requirements in the draft bill renders unnecessary the supplemental layer of regulation that would be created by the FTC under the draft bill. We should avoid creating a new compliance burden that does not offer increased data security.

Provide appropriate enforcement—BSA supports the draft bill's grant of authority to the FTC and State AGs to vigorously enforce to defend consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses. We strongly recommend the inclusion in the bill of a provision explicitly stating that it does not create a private right of action.

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Commerce, Manufacturing and Trade

Hearing on the Discussion Draft of H.R. ___
a bill to require greater protection for sensitive consumer data
and timely notification in case of breach

Testimony of Robert W. Holleyman II
President & CEO, Business Software Alliance

Wednesday, June 15, 2011

Chairman Bono Mack, Ranking Member Butterfield, thank you for holding this hearing today and for inviting me to testify. My name is Robert Holleyman. I am the President and CEO of the Business Software Alliance (BSA.) BSA is an association of the world's leading software and hardware companies. BSA's members create approximately 90% of the office productivity software in use in the U.S. and around the world.[1]

The Business Software Alliance and its member companies strongly support enacting a national data security and data breach notification law, because it is important that we maintain trust and confidence in digital commerce. The time to act is now. This is the fourth Congress to consider such legislation. The need is clear, as are the solutions. We urge you to pass a data security and data breach notification bill this Session.

Over the last 20 years, consumers, businesses and governments around the world have moved online to conduct business, and access and share information. This shift to a digital world has revolutionized personal interactions, education, commerce, government, healthcare, communications, science, entertainment and the arts, etc. It has delivered unprecedented efficiencies and considerable cost savings and it will continue to produce immense benefits to our global society. Looking ahead, into the just-dawning era of cloud computing, these revolutions will only intensify – accompanied by even greater economic and social benefits.

These changes bring with them a number of risks. We all face a variety of online threats, which can undermine trust in the digital environment.

Just ten years ago, the primary threats to security online were vandals and hackers. They chased notoriety and relished the challenge of beating security systems. Their calling cards were breaches, denial of service attacks to bring down popular sites such as eBay and CNN.

But the stakes are now higher: these activities are increasingly motivated by profit. The data mined from breaches can be used to send targeted spam, to impersonate unknowing individuals and steal finances. Increasingly organized criminal enterprises are using the Internet to distribute malware so they can make big money.

BSA commends you for bringing a focus on data security in the digital age. This is a matter of great concern for BSA member companies that engage in electronic commerce and provide much of the infrastructure to make e-commerce possible. Unauthorized disclosures of personal information erode public confidence in the online world. Cloud services are already an important component of how information is developed, managed and stored, and over the coming years we anticipate its importance will grow. But, electronic commerce and cloud computing cannot reach their full potential to contribute to U.S. economic growth without the trust of consumers and businesses. BSA believes that legislation, like the draft bill under consideration today, can be an important component in strengthening trust in the online environment.

[1] The Business Software Alliance (www.bsa.org) is the world's foremost advocate for the software industry, working in 80 countries to expand software markets and create conditions for innovation and growth. Governments and industry partners look to BSA for thoughtful approaches to key policy and legal issues, recognizing that software plays a critical role in driving economic and social progress in all nations. BSA's member companies invest billions of dollars a year in local economies, good jobs, and next-generation solutions that will help people around the world be more productive, connected, and secure. BSA members include Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, Cadence, CNC/Mastercam, Compuware, Corel, Dassault Systèmes SolidWorks Corporation, Dell, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, PTC, Progress Software, Quark, Quest Software, Rosetta Stone, Siemens, Sybase, Symantec, and The MathWorks.

1. **The size and nature of the challenge**

Even as consumers share more of their personal information on line, the security and confidentiality of their personal data is threatened: a recent survey of American adults found 68 percent of them were either "very concerned" or "extremely concerned" about identity theft.[2] Over the past several years, the number of significant security breaches has continued to increase.

- A recently released Ponemon study shows that the average cost of a data breach grew to $214 per record compromised in 2010, up from $204 per record in 2009, while the average security incident cost individual companies $7.2 million per breach in 2010, up from $6.43 million in 2007 and $4.7 million in 2006.[3]
- For the eleventh year in a row, identity theft tops the FTC list of U.S. consumer complaints. Of 1,339,265 complaints received in 2010, 250,854 – or 19 percent – were related to identity theft.[4]
- According to the non-partisan *Privacy Rights Clearinghouse*, data breaches have affected a staggering 533 million records containing sensitive personal information since 2005.[5]

As we look ahead, the vast amounts of information that will be stored in the cloud promise to be alluring targets for cybercriminals.

Illicit activity in connection with the Internet has evolved over the past decade. The history of hacking includes tales of both innocuous white-hatted do-gooders looking to help industry clients as well as malevolent thieves looking to steal information for profit. The hapless employee who carelessly loses – or allows to be stolen – a laptop filled with sensitive information to be stolen can also be the source of a breach.

Determining the actual impact of breaches has been difficult. A recent GAO study noted comprehensive data on the consequences of data breaches does not exist. What is clear and what matters most is that companies must do their best to protect the sensitive information of their customers – and they must respond responsibly when any breach does occur.

Today, though, the response to such attacks is complicated for businesses and confusing for customers because of the patchwork of sometimes conflicting state laws. Federal legislation can help clarify and improve the process and allow industry to do what it does best – focus on improving the security of online systems to prevent future attacks and diminish the harm of any actual breach.

2. **Business response to the data security challenge**

It is clear that organizations that hold sensitive data need to improve their risk management. But this does not necessarily require adopting extraordinary, excessively costly or particularly cumbersome

[2] http://arstechnica.com/security/news/2009/10/americans-fear-online-robberies-more-than-meatspace-muggings.ars

[3] http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

[4] http://ftc.gov/opa/2011/03/topcomplaints.shtm

[5] http://www.privacyrights.org/data-breach

security measures: a study conducted by Verizon, the U.S. Secret Service and the Netherlands' High Tech Crime Unit shows that, in 2010, 83 percent of breached organizations were targets of opportunity, and 96 percent of breaches could have been avoided through simple or intermediate controls.[6] In other words, reasonable diligence could make a considerable dent into this problem.

For its part, the technology industry has important responsibilities to respond to this.

First, each and every day our members focus on the trustworthiness of the information technology products, systems and services. As governments, critical infrastructure providers, businesses and consumers worldwide depend upon these technologies, our members undertake significant efforts to reduce their vulnerabilities, improve their resistance to attack and protect their integrity.

Users can be exposed to cybersecurity risks in a great many ways, including when they use counterfeit or unlicensed technologies. Users of counterfeit hardware or software have no assurance of their trustworthiness, and in many cases intentional vulnerabilities – i.e. malware –are found in counterfeits.[7]

Second, our members work diligently to develop security technologies to defend against evolving threats. Users of technology rely on BSA members for innovative solutions that provide layered defenses – from protection at the data and document level to the network and perimeter level – that are adapted to the threats they face and the value of the assets they need to protect.

And finally, our members educate and raise public awareness of cyber risks and how users can protect themselves. Many of our members have developed their own substantial programs to convey these messages, and many offer free security checkup tools. In addition, several BSA members play a leading role in the National Cyber Security Alliance (NCSA),[8] a non-profit organization supported by public and private sector partners. NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school.

3. Objectives of federal data security and breach notification legislation

BSA believes federal legislation that requires organizations to secure the sensitive personal information they hold, and to notify individuals when that security has been breached, can effectively enhance consumers' trust. Federal legislation establishing a uniform national framework would benefit businesses and consumers alike. It would replace state laws that are generally good, but that are now creating confusion and difficulties. This uniformity would best serve the interests of businesses, but it is important to note that it would also best serve those of consumers by guaranteeing a high level of protection not just in the response to a breach, but also in its prevention.

BSA recommends that federal data security and breach notification legislation pursue the following objectives, which we are pleased to see reflected in the draft bill.

---

[6] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

[7] See for example the 2006 IDC White Paper on "The Risks of Obtaining and Using Pirated Software." It showed that 25% of the Web sites that were reviewed for the study that offered counterfeit product keys, pirated software, key generators or "crack" tools attempted to install either malicious or potentially unwanted software. It also showed that 11% of the key generators and crack tools downloaded from Web sites and 59% of the key generators and crack tools downloaded from peer-to-peer networks contained either malicious or potentially unwanted software.

[8] http://www.staysafeonline.org

Establish a uniform national standard that preempts state laws

The National Conference of State Legislatures (NCSL) indicated that, as of October 2010, forty-six States, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands had enacted data breach notification laws.[9] This patchwork has created a compliance nightmare for businesses. As businesses may in good faith comply in different ways, this in turn creates confusion for consumers who receive notices from a multiplicity of sources.

For example, most state laws exempt encrypted data from the obligation to notify because they rightly consider that such a breach does not create a risk of harm. However, some jurisdictions including the District of Columbia, Wisconsin and New Hampshire require notification even when the data was encrypted. This jeopardizes the legal benefit for businesses of encrypting data. It also creates the likelihood that residents of other states will get notified even if their data was encrypted, and thus even if they are not at risk.

We are heartened by the draft bill's inclusion in section 6 of language pre-empting state laws, and suggest that the scope of preemption be clarified to cover notification to government agencies as well as private parties.

Prevent excessive notification

Not all breaches are of equal importance. Some create great risks of harm to consumers from identity theft and fraud, while other breaches create little to no risk. Currently, most state data breach laws require notification in all instances, even when no risk results from the breach. Over notification is likely to confuse consumers, who will then fail to take appropriate action when they are truly at risk.

We believe notification should be required only in those instances where an unauthorized disclosure presents a significant risk of material harm. We are pleased that section 3(f) of the draft bill takes a risk-based approach to breach notification. We recommend that the threshold be *"significant risk,"* to ensure that only genuine risk is notified.

Exclude data that has been rendered unusable, unreadable, or indecipherable

We also recommend that data not be subject to breach notification if it has been rendered unusable, unreadable, or indecipherable through practices or methods, such as encryption, redaction, or access controls, which are widely-accepted as effective industry practices or industry standards.

These conditions will ensure that data that has been illicitly accessed cannot actually be used to defraud or inflict harm on data subjects. As the apparent breach would not pose a risk to the consumer, it should not require notification. Such an exemption would also be technology neutral and flexible, allowing innovators to continue to develop new techniques and methods without fearing that legislation and regulations have favored one type of measure over another.

The draft bill's section 6(f)(2) provides a market-based incentive for the adoption of strong data security measures. We recommend however that this provision be made technology. As drafted, we are

[9] http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

concerned that it may tilt the playing field by setting up a two-tiered approach: while encryption is explicitly listed in the draft bill, other methods would require the sanction of an FTC rulemaking. This would put the FTC, which may not have the adequate technological or business expertise, in the difficult position of deciding what technologies are sufficiently secure to protect what types of data in what environment. In any case, the need for an innovating company to obtain this FTC sanction, before it can convince potential customers that they can use a new technology or method, is likely to chill such innovation.

We recommend that the legislation itself provide an exemption, for unusable, unreadable or indecipherable data, that is available to any widely-accepted effective industry practice or industry standard. The vigilant oversight of the FTC will ensure that the marketplace continuously adapts to *"effective industry practices or industry standards."*

Require the use of data security safeguards

Requiring breach notification is fair to consumers who need to know they are at risk. We believe, however that more can be done to prevent breaches from happening in the first place, by requiring organizations that hold sensitive personal information to establish and implement data security policies and procedures. We support the fact that the draft bill does this in section 2.

Such a requirement should be flexible, reasonable and appropriate, and take into account the size, scope and nature of the organization's activities and the cost of implementing safeguards.

We think it would be appropriate to deem in compliance with the draft bill's data security requirements those organizations that comply with recognized industry standards for data security risk management. Such standards include ISO/IEC 27001, the Standard of Good Practice of the Information Security Forum, or the COBIT framework created by the Information Systems Audit and Control Association (ISACA.) This would simply extend to recognized industry standards the safe harbor created by the draft bill in section 2(a)(3), which applies to organizations whose data security obligations are already regulated by other federal laws with equivalent requirements.

It is particularly important to avoid imposing technology mandates. Organizations must be able to deploy appropriate and cutting edge security measures and technologies to effectively protect themselves and their customers' sensitive data against current and future threats. This would not be possible if the law mandated the use of specific products or technologies. Laws and regulations should focus instead on requiring the implementation of reasonable and appropriate security measures. We are pleased that section 4(b)(3) of the draft bill bars the FTC from *"requir[ing] the deployment or use of any specific products or technologies, including any specific computer software or hardware."*

It is also important to avoid over-regulating data custody. While we support the draft bill's requirement that organizations protect the consumer data that they hold, we are concerned that the grant of authority to the FTC, in section 2(a)(1), to develop a body of regulations governing such corporate policies and procedures will in effect make the activity of data custody a regulated activity. The specificity of the data security requirements in the draft bill, and the existence of industry standards for data security risk management – such as ISO/IEC 27001, the Standard of Good Practice, or COBIT – render unnecessary the supplemental layer of regulation that would be created by the FTC under the draft bill. We should avoid creating a new compliance burden that does not offer increased data security.

We believe that the FTC enforcement actions will be sufficient to ensure that effective action is actually taken by companies to secure their systems and data.

Provide appropriate enforcement

Legislation should ensure that vigorous enforcement can take place to defend consumers against businesses that fail to provide fair protection of sensitive personal data, without interfering with legitimate businesses.

The FTC has a strong track record in that respect, and BSA supports the draft bill granting to the FTC powers of enforcement in section 4(b).

We also support the inclusion of state Attorneys General as enforcers when the FTC has not acted. We support the draft bill's requirement, in section 4(c), that state AGs bring their civil actions under the bill in federal court. Federal jurisdiction will improve consistency in the application of federal legislation throughout the country.

BSA believes it is also important to prevent excessive litigation. The judicial system is not a desirable forum to determine the adequacy of data security measures. Moreover, allowing private lawsuits as a result of the occurrence of a data breach would create the risk that some data custodians refrain from notifying consumers in case of breaches, for fear of opening themselves to lawsuits. Therefore, we strongly urge you to include a provision explicitly stating that nothing in the draft bill is a basis for a private right of action for damages, as the Administration has proposed.

Mrs. BONO MACK. Mr. Pratt, you are recognized for your 5 minutes.

STATEMENT OF STUART K. PRATT

Mr. PRATT. Madam Chairman, Ranking Member Butterfield, and members of the subcommittee. My name is——

Mrs. BONO MACK. Excuse me, is that microphone on?

Mr. PRATT. It is. I will pull it closer.

Mrs. BONO MACK. Thank you.

Mr. PRATT. Madam Chairman—is it working?

Mrs. BONO MACK. If the light is on. I can't necessarily tell, but the people in the back really care that they will hear well.

Mr. PRATT. I am President and CEO of the Consumer Data Industry Association. We appreciate the opportunity to testify today.

For more than a decade, CDIA has been on record as supporting the enactment of a inform Federal standard for both security of sensitive personal information and notification of consumers where there is a significant risk of identity theft.

With this in mind, we applaud the focus of this hearing. Your committee's leadership is key to finding the right path forward. CDIA's members support the proactive approach you have taken by circulating a discussion draft in order to build the much-needed consensus. It is the right step to take.

You have asked us to comment on the discussion draft known as the SAFE Act, or SAFE Data Act. So, first, CDIA is very encouraged by the essential structure of the draft bill. Risks to sensitive consumer data are best addressed with two key pillars:

First, sensitive personal data must be secured. The draft proposal appropriately empowers the Federal Trade Commission to write scalable regulations relative to data security, much as the FTC and bank agencies have done for financial institutions governed by the Gramm-Leach-Bliley Act. CDIA members support this approach.

Second, consumers must be notified when sensitive personal information about them has been lost or stolen. Again, our member support notification where, for example, there is a significant risk of harm for the consumer, such as the likelihood of becoming a victim of the crime of identity theft.

Within these two key pillars are many provisions which are well thought out and deserve to be highlighted. For example, the discussion draft establishes strong incentives for U.S. businesses to adopt strategies to reduce risks by rendering data unusable, unreadable, orindecipherable. These incentives are appropriately technology-neutral and thus will spur innovation in the design of systems that will ultimately protect data about consumers.

The draft properly includes a risk-based trigger for determining when a notice must be sent, which ensures that we as consumers receive relevant and timely notices, rather than a deluge of notices through which we need to sift to find the one that is meaningful.

While the draft urges speedy notification of consumers, it acknowledges the need for law enforcement to engage with private sector and, in some cases, to delay such notices, but not to allow delays that are unduly long.

We are pleased that the draft's proposals solve the problem of overlapping laws with regard to data security. Fully exempting persons who are subject to the data security requirements of Title 5 of the Gramm-Leach-Bliley Act ensures that CDIA members, both large and small, are in the very best position to successfully comply with the law and, most importantly, to be successful in securing sensitive personal information about consumers.

We encourage the committee to adopt a similar subject to standard with regard to persons who are already held accountable for data breach notification duties under Federal laws, regulations, or agency guidance.

Ensuring a truly uniform national standard for both data breach notification and data security is essential to the success of the draft the proposal. To this end, we applaud the inclusion of section 6. As the committee continues to refine the discussion draft, we encourage it to consider a subject matter approach to preemption to ensure that the standard is truly uniform.

Regarding the content of notices, let me make just a couple of points:

First, we thank you for the inclusion of language in section 3(e), which makes it clear that the person who experienced the breach and who is notifying consumers is the one who pays for the credit reports to which the consumer is entitled.

Second, for the sake of consumers, we request that the bill be amended to require those who are sending out breach notices to more than 5,000 individuals, to notify consumer reporting agencies in advance so that our members can appropriately prepare to handle the spike in volume.

Further, all persons issuing notices must verify the accuracy of the contact information included. Our members have at times discovered that breach notices issued by others had incorrect toll-free numbers listed, which is a disservice to consumers.

In terms of definitions, we are glad that section 5(7)(A) establishes the definition for the term "personal information." Having a definition is clearly necessary to ensure that all persons affected by the scope of the bill understand the type of data which must be protected. Section 5(7)(B) properly excludes public records from that definition.

Our members are concerned with the inclusion of section 5(7)(C) which allows the FTC to alter the definition. We believe the definition as proposed is adequate and should be set by the Congress.

In closing, let me congratulate you on a very strong discussion draft that is unencumbered by ancillary issues. The committee is on the right track, and we look forward to supporting its efforts to protect consumers' sensitive personal information. Thank you.

Mrs. BONO MACK. Thank you, Mr. Pratt.

[The prepared statement of Mr. Pratt follows:]

STATEMENT OF

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

BEFORE THE

Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade

House of Representatives

ON

Discussion Draft of H.R. ___, a bill to require greater protection for sensitive consumer data and timely notification in case of breach

Wednesday, June 15, 2011

1090 Vermont Avenue, NW, Washington, D.C. 20005

202-371-0910 Phone 202-371-0134 FAX

Chairman Bono-Mack, Ranking Member Butterfield, and members of the Subcommittee, my name is Stuart Pratt, and I am president and CEO of the Consumer Data Industry Association (CDIA). Thank you for this opportunity to testify.

CDIA is an international trade association with more than 190 member companies, providing our nation's businesses with the data tools necessary to manage risk in a wide range of consumer transactions. These products include credit and mortgage reports, identity verification tools, law enforcement investigative products, fraudulent check transaction identification systems, employment screening, tenant screening, depository account opening tools, decision sciences technologies, locator services and collections. Our members' data and the products and services based on it, ensure that consumers benefit from fair and safe transactions, broader competition and access to a market which is innovative and focused on their needs. We estimate that the industry's products are used in more than nine billion transactions per year.

We applaud the focus of this hearing. For more than a decade CDIA has been on record as supporting the enactment of a uniform Federal standard for both the security of sensitive personal information and the notification of consumers where there is a significant risk of identity theft.

You have asked us to comment on the discussion draft H.R. – entitled the "Secure and Fortify Electronic Data Act" (SAFE Data Act). While CDIA will continue to analyze this proposal, below are selected thoughts which we hope will be helpful to you and the

Committee as you continue to refine the bill. We look forward to continuing this dialogue beyond today's legislative hearing.

Alignment of H.R. – with existing state and Federal laws:

Section 2 of the draft bill proposes to require any person engaged in interstate commerce that owns or possesses data in electronic form containing personal information to establish policies and procedures for information security based on rules which would be promulgated by the Federal Trade Commission. Section 3 of H.R. - requires these same persons to comply with specific requirements of the Act where they discover a breach of security relating to personal information.

First, it is essential that these two duties (securing information and notification in the case of a data breach) are fully and completely preemptive of any current or future state laws that address in any way the same subject matter. With this in mind, we generally applaud the inclusion of Section 6 dealing with preemption. In terms of details, we will look over the provision in greater detail and likely provide some additional suggestions to ensure that the intent of this section is accomplished.

Regarding the data security component of the bill, section 2(b) is an excellent start in terms of ensuring that H.R. – does not impose duplicative standards on U.S. businesses that are already subject to duties in other Federal laws. CDIA fully supports the clear and complete exemption for persons who are subject to the Gramm-Leach-Bliley Act with

regard to duties to secure sensitive personal information. This clear exemption is the right statutory construction. We would suggest expanding this exemption to include consumer reporting agencies that are subject to the Fair Credit Reporting Act (15 U.S. C. 1681 *et seq.*).

Regarding the breach notice component of the bill, we suggest that the same statutory construction of the data security exemption be used with regard to Section 3(j). Section 3(j) appears designed to avoid duplicative duties for persons who must provide a notification to consumers under other Federal laws where there has been a breach of sensitive personal information. We believe the bill's "in compliance with" standard, however, does create a problem of double-jeopardy for companies subject to other laws or Federal regulations. We look forward to continuing a dialogue on this provision and appreciate the inclusion of language on this subject.

Align duties and enforcement -

Section 4 of H.R. – applies the requirements of Sections (2) and (3) to any person in possession personal information as defined by the bill. We will continue to analyze this question, but our first-impression is that the broad application of these requirements appears to create tension between the application and the exemptions to these requirements established in sections 2(b) and 3(j), discussed above. We would like to work with your staff to clarify that these questions are addressed.

We would also want to further examine the references to the term "information broker," and how that definition may be duplicative of the general application of the draft legislation.

Let me now discuss some of the ways in which duties under H.R. - interplay with existing duties found in other laws.

Data Breach Notification Requirements

Section 3 of H.R. - establishes requirements for notifying consumers where there is a breach of personal information. A notice is not required where "there is no reasonable risk of identity theft, fraud, or other unlawful conduct." There are also exceptions to the notification requirement if the data was encrypted or otherwise rendered unreadable or indecipherable.

CDIA agrees that an effective risk-based trigger for the disclosure of notices is necessary and believes that the phrase "significant risk of identity theft" sets the right standard. We also agree that there should be specific exceptions for data which is encrypted or otherwise rendered unreadable, indecipherable or unusable.

Timing of breach notification

We agree that law should set clear parameters with regard to the timing of when notices should be sent to consumers. Currently H.R. – proposes that notices should be sent within 48 hours. CDIA will continue to consult with its members to provide additional input on this requirement and whether or not there are consequences to this approach. We would urge the committee to also consider consultation with law enforcement agencies which sometimes need additional investigative time to fully understand the nature of the breach and the risks to consumers.

Content of Breach Notifications

Section (3)(d)(B) describes the content of notices which will be sent to consumers. With regard to the consumer's right to one free credit report on a quarterly basis, we appreciate inclusion of the language in Section 3(e) which makes it clear that the person who experienced the breach and who is notifying consumers is the one who pays for the credit reports to which the consumer is entitled.

3(d)(B)(iv) requires that the toll-free numbers for major credit reporting agencies be included in the notice. We request that the bill be amended to require those who are sending out breach notifications to more than 5,000 individuals to notify the consumer reporting agencies in advance, so that our members can appropriately prepare to handle the spike in volume. Further, all persons issuing notices must verify the

accuracy of the contact information included. Our members have at times discovered that breach notices issued by others had incorrect toll free numbers listed, which is a disservice to consumers.

Definition of Personal Information

Section 5(7)(A) establishes a definition of the term "personal information." Having a definition is clearly necessary to ensure that all persons affected by the scope of the bill understand the type of data which must be protected. Our members are concerned with the inclusion of Section 5(7)(B) which allows the FTC to alter this definition. We believe the definition as proposed is adequate and should be set by Congress. The FTC could make a determination that a new element of data is now included under the definition and in doing so unintentionally cause extraordinary expense for affected persons. As written the FTC is not required to validate their reasons for changing the definition, nor are they required to determine the financial or product impact such a change would have.

Enforcement

CDIA continues to believe that enforcement of the statute by state attorneys general should be comparable to the FCRA provision which allows them to sue for actual or statutory damages of $1,000 for each negligent or willful violation (see FCRA Section 621(c)(1)(B)). We believe a cap on damages is also appropriate and that compliance with the provisions of this Act should be tied to a "reasonable procedures" standard.

Uniform National Standard

As discussed above, CDIA applauds the inclusion of language in Section 6 which proposes to preempt additional state actions. Our members believe that absolute uniform standards are critical if this bill is to become law and we are happy to provide additional input on the current provision, which appears to be construed too narrowly.

Conclusion

Again, thank you very much for the opportunity to testify. I am happy to address any questions that you may have.

Mrs. BONO MACK. Mr. Rotenberg, 5 minutes.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Thank you, Madam Chair, Mr. Rush, members of the committee. My name is Mark Rotenberg. I am the Executive Director of the Electronic Privacy Information Center, and I teach privacy law at the Georgetown Law Center, and I thank you very much for holding this hearing today.

It is actually difficult to overstate the problem of security breaches in the United States. In fact, as your earlier hearings have demonstrated, these risks are far-reaching and they impact millions of consumers,, in May, more than 200,000 customers of Citigroup, and 100 million users of the PlayStation Network also had information improperly accessed.

And if I can make an additional point for you this morning, these problems are going to get worse. We are moving more of our personal data from our laptops, our devices, and our desktop computers into the cloud where they can be more easily accessed by others. You are going to hear more and more about security breaches.

You are also going to learn that the attacks are becoming more sophisticated. Not only do we have to now contend with phishing, which seeks to obtain sensitive personal data, we now have to contend with what is called spear phishing, which means identifying particular users and using some information about them, such as their home address, to get additional information that makes possible identity theft, financial fraud, and so forth.

So at the outset, my sense would be that given the fact that the House last year had passed a strong measure, the problems are getting worse and likely to continue to do so. I would have started there and tried to figure out how to improve that bill. And in that spirit, I actually wanted to commend you for incorporating the data minimization provision in the draft bill.

I think this is a very important safeguard that not only limits the risk at the outset by telling companies, you know, really think if you need to have Social Security numbers on health club members, for example, because if you lose control of that information, you have created a risk. So you reduce the risk at the outset. But in the circumstances where the information isn't properly accessed, there is less exposure to customers, so that is also an important safeguard. And I am very glad to see that incorporated in the draft measure that you circulated, as well as the effort to reduce the time period for notification.

Because one of the other things that we have learned based on the Citibank experience and the Sony experience is not surprising. These companies are reluctant to notify their customers when they have a problem, and that is why legislation is so important for companies to tell customers that there is a problem and that you are going to need to act on this information. So I think the fact that you have limited that time period is very important.

Now, in my written testimony, I made some additional suggestions, and I will try to highlight the key points in particular about questions that have been raised by the members during the earlier part of this hearing with Commissioner Ramirez.

I noticed for example, Dr. Cassidy had asked this question: Well, why should we have a public information, you know, requirement if that data is already out there? Can't we kind of put that in a separate category and not have to notify people? And I think the answer is obvious.

There is a big difference between someone breaking into a database to get someone's home address and someone finding the home address in a publicly accessible file. And the reason, of course, is that there is intent behind the break-in to go after the person whose home address has been obtained. And the fact that it might be accessible somewhere else should hardly make people feel good about the fact that it can be categorized as public information.

So I would take away that exception that says that somehow companies get a free pass if it is information that can be obtained somewhere else, and therefore they don't have to worry about people breaking in who get access to it. I think the home address information makes obvious the problem.

There has been some discussion about how do we define personally identifiable information. It is a very difficult problem. It comes up in almost every privacy bill. I think a very good starting point is to say, simply, personally identifiable information is information that identifies or could identify a person, and then include by way of illustration, including but not limited to many of the provisions you have in your bill. So it is a Social Security number, it is a bank account number, it is a person's name, it is a home address. But it could also be an IP address; in other words, the fixed Internet address associated with their laptop or their mobile device. That very well could be personal identifiable information.

Their Facebook user ID could also be personally identifiable information. In fact, that is exactly what contributed to one of the concerns about app access to Facebook-based information.

On this critical question of preemption, I completely understand why my colleagues at this table would favor national standard. It is quite sensible from their perspective. But I would urge you to look very closely at some of these strong State measures that would be effectively overwritten if a weak Federal standard is established.

Those bills are important, and even in States like California, where they thought they had it right the first time on financial data, they had to come back later and deal with medical breach notification as well.

Thank you very much.

Mrs. BONO MACK. Thank you, and I apologize that I did not pronounce your name correctly. Mr. Rotenberg. Correct?

Mr. ROTENBERG. Thank you.

Mrs. BONO MACK. Thank you.

[The prepared statement of Mr. Rotenberg follows:]

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on the Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach

Before the

House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

June 15, 2011
2322 Rayburn House Office Building
Washington, DC

Madame Chair and Members of the Committee, thank you for the opportunity to testify today on the SAFE Data Act. My name is Marc Rotenberg. I am executive director of the Electronic Privacy Information Center ("EPIC") and I teach privacy law at Georgetown University Law Center.

We are grateful for the work of this Committee on the critical issue of data security and privacy protection. In my testimony this morning, I will discuss the urgency of this problem, review the proposed legislation, and make a few further points about forward-looking strategies for privacy protection.

I also want to acknowledge two organization that have expressed support for this statement: the Consumer Federation of America and the U.S. PIRG. I would encourage the members of the Committee and their staff to communicate directly with these groups as the legislative process moves forward.

One key point to make at the outset is that almost all of the states have responded over the last few years to develop robust security breach notification legislation. Many of these laws can be traced back to the California notification law that was famously triggered in a matter that EPIC brought attention to involving the sale of data on American citizens to a criminal ring engaged in identity theft. That notification and the investigation that followed led to dramatic changes in the information broker practices in the United States. While there is clearly a lot more that needs to be done to safeguard personal data, you should not underestimate the enormous value of these breach notification statutes as well as the unintended problems that could result if federal law preempts more responsive state laws. For reasons I will discuss in more detail below, I recommend that you not adopt legislation that would preempt the ability of the states to develop more effective means to respond to these new problems.

Scope of the Data Breach Problem

In recent months, there have been a large number of high profile data breaches that illustrate the severity of the problem and necessity of comprehensive data breach legislation.

- A recent breach at Southern California Medical-Legal Consultants, a company representing medical providers for workers' compensation claims, disclosed personal data, including names and social security numbers, of approximately 300,000 people.[1]

[1] Press Release, Southern California Medical-Legal Consultants, Possible Data Breach Discovered and Contained (June 11, 2011), http://www.scmlc.com/press.htm.

- In May, a breach at Citigroup exposed customer names, account numbers, and contact information for more than 200,000 customers. Citigroup waited almost a month before it notified its customers.[2] Experts have warned that this disclosure of customer data will make Citigroup customers especially vulnerable to phishing attacks and other acts of fraud.[3]

- The PlayStation Network breach in April exposed personal data, including names, addresses, passwords, and possibly credit card data, of over 100 million users.[4]

- A breach at Epsilon, an internet marketing company, in late March, disclosed personal information, including names and email addresses, of millions of consumers.[5]

According to the Identity Theft Resource Center, there have been at least 195 data breaches in 2011.[6] In 2010, there were 662 breaches and over 16 million records compromised.

These problems are going to get worse. As more sensitive data moves into the cloud, as we become more dependent on electronic health records, and more companies store vast amounts of consumer data on remote servers, the risk that personal data will be improperly disclosed or accessed will necessarily increase.

Moreover, consumers and businesses that become increasingly dependent on these services are less likely to know when problems occur than if they were to lose their own laptop or experience a break-in.

Breach notification does not solve these problems. But it does help us to understand the extent of the problems so that better safeguards and practices can be developed.

---

2 Randall Smith, *Citi Defends Delay in Disclosing Hacking*, Wall St. J. (June 13, 2011), http://online.wsj.com/article/SB10001424052702304665904576382391531439656.html

3 Jeremy Kirk, *Citigroup Breach Exposed Data on 210,000 Customers*, PC World (June 9, 2011), http://www.pcworld.com/businesscenter/article/229868/citigroup_breach_exposed_data_on_210000_customers.html.

4 Liana B. Baker & Jim Finkle, *Sony Playstation Suffers Massive Data Breach*, Reuters (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

5 Hayley Tsukayama, *Sony, Epsilon Support National Data Breach Bill*, Wash. Post. (June 3, 2011), http://www.washingtonpost.com/blogs/post-tech/post/sony-epsilon-support-national-data-breach-bill/2011/06/02/AG34tvHH_blog.html.

6 As of June 7th, 2011. The report also lists 11,030,619 records being compromised but does not include the record counts for the most recent data breaches. Identity Theft Resource Center, 2011 Data Breach Stats 7 (June 7, 2011), http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202011.pdf.

Structure of the SAFE Data Act

Section 2 of the SAFE Data Act sets forth new Data Security Requirements that require companies to assess and address vulnerabilities within their systems and participate in data minimization practices.

Section 3 of the SAFE Data Act includes provisions on data breach notification that create deadlines for notification of law enforcement and consumers. Law enforcement must be notified within 48 hours of discovery. Companies must assess the scope of the breach, identify the nature of the breach, and address the vulnerabilities that created the breach. Within 48 hours of conducting this assessment, companies may have to notify consumers.

Section 3, the Application and Enforcement section of the SAFE Data Act, allows for enforcement by the Federal Trade Commission and state attorneys general. It does not provide for a private right of action or statutory damages scheme.

Section 6 of the SAFE Data Act, entitled Effect on Other Laws, includes a provision that states that this bill would preempt all state information security laws generally and state created civil actions for data breach specifically.

Important Changes from Earlier Bill

The SAFE Data Act is based on similar legislation that has been considered and favorably reported by this Committee in the past. There are two significant changes in this bill that we support.

First, we support the data minimization provision. It has become clear that one of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks do occur is to collect less sensitive personal information at the outset. It is the credit card numbers, the bank account numbers, the social security numbers, and the passwords that draw the attention of computer criminals. Reducing the target size reduces the vulnerability.

On data minimization, we would urge you to go further. Instead of simply a data minimization plan, we would recommend a data minimization requirement. There are many examples of this already in privacy law. For example, the Video Privacy Protection Act requires businesses to:

> Destroy personally identifiable information as soon as practicable, but not later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pendin requests or orders for access to such information . . .

Other privacy bills include similar requirement.[7]

[7] *See e.g.* Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services

The simple message to business should be "if you can't protect it, don't collect it."

Second, we support the 48-hour requirement for breach notification. Earlier versions of the bill allowed companies to wait 7 days, in some instances 60 days, before notifying those whose personal data was compromised. That is too long. The shorter time period will require companies to respond quickly when there is a problem. This shorter period will also allow consumers to react more quickly and take preventative or mitigating actions.

Additional Improvements

Method of Notification

The bill currently proposes the use of either written notification or email notification when an obligation to provide notification arises. I would suggest that you include an additional obligation to provide a text message where possible. A text message would not be an effective substitute for written notification or email, because it is essentially ephemeral. But is a very effective technique for notification and it could help make people aware that they should look for a notice that might arrive in the mail or show up in the email box.

In a similar spirit, where the bill speaks of providing notification by means of a web site, it may be appropriate to add "or social network presence." Many organizations today are interacting with users though popular social network services such as Facebook. In many configurations, the data remains with Facebook, so there is no direct data collection by third parties. But in other circumstances, for application developers and advertisers for example, third party companies obtain information from users through Facebook. If security breaches arise in these circumstances, notification by means of the social network service may be the most effective way to reach the target population.

Public Record Defense

The definition of "personal information" in the bill expressly exempts "public record information" available from federal, state, or local government systems and was acquired by the company that suffered the breach for such purposes. The theory underlying this provision, I imagine, is that there could be no additional harm to the individual of the breach of this information if it is already available to the public. But this is the wrong way to understand the problem and the affirmative defense will undercut the purpose of the bill.

If an organization suffers a security breach of confidential information or of "public information" it has a problem that needs to be corrected. If no action is taken to

---

Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. §§ 6801, 6809, 6821, and 6827).

correct the problem, it is quite likely the breach will occur again. That is why the security obligation should apply even when there is no immediate harm to the individual: The problem remains. Also, I would not assume the fact that personal information may be found through public data sources that the information disclosed in a data breach is equivalent. It is quite likely, particularly in the information broker industry, that the "public" information contained in a particular data record is far more detailed than any record that would be available in a singe government record system.

Treatment of Personally Identifiable Information

One of the key provision of the bill is the definition of "Personal Information." This definition is critical because, as with most privacy bills, this definition will determine when the obligations of the Act should be applied and when they can be pretty much ignored.

As currently drafted, the bill sets out a narrow definition for Personal Information, as compared with other privacy statutes. For example, the bill seems to suggest that a social security number would not be personally identifiable if it is possessed without the associated person's name. The bill also ignores other popular identifiers, such as a user ID for Facebook, which points as readily to a unique individual as would a driver's license or a social security number.

The definition is also narrow in light of the 2009 FTC on Internet advertising that noted that there are many ways to track Internet users, including the use of "IP address" that can uniquely identify a user's computer, much as phone number will uniquely identify a cell phone. In many cases, this is also a form of personal information that should be subject to the bill's requirements.

I would suggest a construction that would define Personal Information as information that "identifies or could identify a particular person," followed by the examples cited in the bill as illustrations, with the qualifying phrase "including, but not limited to." This approach is technology neutral, less dependent on the rulemaking process, and more likely to adapt over time.

Strengthen Notification

The bill addresses preemption and the circumstances under which the federal law would overwrite possibly more effective state information security legislation. As currently drafted, the bill preempts state laws that either have similar security obligations as well as state laws that provide for security breach notification. The bill does leave in place state trespass, contract and tort law, as well as claims involving fraud.

My own view is that it would be a mistake to adopt a preemption provision of this type. Businesses understandably will prefer a single national standard. That is the argument for preemption. However privacy laws have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish. This approach to

consumer protection is based upon our federalism form of government that allows the states to experiment with new legislative approaches to emerging issues.

The breach notification provision should be strengthened and clarified. The bill states that if the company determines that there is no "reasonable risk of identity theft, fraud, or other unlawful conduct" the notification of customers is not required. The bill should be modified to make clear that it imposes a presumption in favor of notification. The ability to assess the risk and make a decision about breach notification should not rest in the hands of the entity that allowed the breach to occur. We recommend that the right to assess the severity of the breach be placed in the hands of either an independent regulatory agency (the Federal Trade Commission) or the consumers. Routine notification should be required.

As we have explained in previous testimony,[8] identity theft is only one risk from unauthorized access to personal information. Unauthorized access may be gained for other purposes that cause harm to the individual, such as stalking, obtaining information for debt collectors, corporate espionage, extortion, or to supply information that will be used for future phishing or fraud activities. The recent breach at Citigroup is a good example of this. The information originally obtained in the breach may not have included social security numbers, credit card numbers, or other traditional tools of identity theft, but it was enough to leave consumers vulnerable to phishing attacks. In instances such as this, consumers should be notified so that they can take proper precautions against future attacks and possible fallout from the data breach.

In other circumstances, a reasonableness standard might be appropriate. The problem here is that the company will decide itself, having suffered the breach, *whether there is reasonable risk of harm to others* and there will be no effective way to review this decision if the company guesses wrong. That is an approach that will invite greater secrecy and less accountability. Companies often cannot tell whether a security breach may result in identity theft. The motives of a person who gained access are not always clear. Identity theft can also occur months or even years after a security breach.

Placing the decision about whether or not to notify customers in the hands of the company is also problematic because companies are often reluctant to disclose breaches to customers. Sony, for instance, waited a week to notify customers of its data breach.[9] Citibank waited a month. [10]

Because it is difficult to gauge the risk of identity theft, because there are harms other than identity theft which may result from security breaches, and because there is already evidence that companies will go to great lengths to avoid giving security breach

---

[8] EPIC, *Testimony for the Legislative Hearing on "Data Security: The Discussion Draft of Data Protection Legislation"*(July 29, 2005), http://epic.org/privacy/choicepoint/datasec7.28.05.html.

[9] Missouri Attorney General Chris Koster, *Attorney General Koster Says Sony Failed to Warn Consumers About Playstation Network Breach,* Attorney General's News Release (April 28, 2011), http://ago.mo.gov/newsreleases/2011/AG_Koster_says_Sony_failed_to_warn_consumers/.

10 Randall Smith, *Citi Defends Delay in Disclosing Hacking*, Wall St. J. (June 13, 2011), http://online.wsj.com/article/SB10001424052702304665904576382391531439656.html

notices, we recommend eliminating the language that gives companies discretion not to give notice based on a determination whether the breach "may result in identity theft."

Private Right of Action

We support the inclusion of provisions allowing enforcement by the Federal Trade Commission and state attorneys general, but would recommend expanding this to include a private right of action for customers. It is often difficult to place a dollar value on data breaches and privacy infringements, so it is important that this private right of action also include a statutory damages provision. This would empower consumers to enforce the law themselves and create a strong disincentive for the irresponsible handling of consumer data. Not only would this provide the opportunity for individuals who have been harmed by security breaches to have their day in court, it would also provide a necessary backstop to the current enforcement scheme which relies almost entirely on the Federal Trade Commission, acting on its own discretion and without any form of judicial review, to enforce private rights.

For these reasons, many state laws include private right of action provisions. California, Hawaii, Louisiana, and Washington, for instance, include provisions in their state data breach laws that allow consumers to bring a civil action and recover damages.[11]

Avoid a Federal "Ceiling" on Breach Notification

We also recommend that the preemption clause in the bill be dropped or modified so that this federal bill creates a "floor" instead of a ceiling. It is important that states be permitted to legislate in this area. As discussed already, most states have comprehensive data breach legislation. Often, this legislation establishes a private right of action, statutory damage scheme, and notification requirements. [12]

Because states enjoy a unique perspective that allows them to craft innovative programs to protect consumers, they should be permitted to continue to operate as "laboratories of democracy" in the privacy and data security arena. State legislatures are closer to their constituents and the entities they regulate; they are the first to see trends and problems, and are well-suited to address new challenges and opportunities that arise from evolving technologies and business practices. This is why privacy bills have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish.

There is an additional reason that we believe weighs against preemption in the information security field: these problems are rapidly changing and the states need the ability to respond as new challenges emerge. California and Massachusetts have recently considered updating their data breach legislation in response to new threats.[13] It is very

[11] Cal. Civ. Code 1798.82 (2011), Haw. Rev. Stat. § 487N-2 (2011), La. Rev. Stat. § 51:3071 et seq.(2011), Wash. Rev. Code § 19.255.010, 42, 56, 590 (2011).
[12] *See e.g.* Cal. Civ. Code 1798.82 (2011).
[13] Jason Gavejian, *California and Massachusetts Legislatures Push Data Breach and Security Bills,*

likely that the states will continue to face new challenges in this field. Placing all of the authority to respond here in Washington in one agency would be, as some in the security field are likely to say, a "critical failure point." The temptation to establish a national standard for breach notification should be resisted, particularly given the rapidly changing nature of the problem.

Looking ahead

While it is clearly important to inform individuals when their personal information in the possession of others has been improperly accessed or disclosed, it is time to ask whether the remedies that are provided are effective or meaningful. Consumers have become increasingly frustrated by the breach notifications that encourage them to sign up for credit monitoring services. Why should they bear the burden for the mistakes of others?

A number of states have recognized that at least part of the solution is to change the default setting for the disclosure of credit data. Laws that "freeze" the disclosure of the credit information pending a choice of the consumers to release simply establish an opt-in that is the commonsense approach for disclosing sensitive personal data.

Conclusion

Data breaches remain one of the greatest concerns for Internet users in the United States. Many companies have poor security practices and collect far more information than they need or can safeguard. But since there are few consequences for poor security practices, they can obtain all the value from the user data and leave it to the consumers to deal with the consequences.

Consumers are also often left out of the loop when breaches occur. They are not informed that their data has been disclosed, so they cannot take mitigating actions to try to minimize the damage. It is important that this problem is corrected with a strong notification requirement. The SAFE Data act should also empower consumers with a private right of action and statutory damages.

Companies need to know that they will be expected to protect the data they collect and that, when they fail to do so, there will be consequences. Legislation for information security and breach notification is needed, but it should not preempt stronger state measures and it should not rely solely on FTC rulemaking authority.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

Workplace Privacy, Data Management, and Security Report (May 3, 2011), http://www.workplaceprivacyreport.com/2011/05/articles/workplace-privacy/california-and-massachusetts-legislatures-push-data-breach-and-security-bills/

Mrs. BONO MACK. As a student of how John Dingell does his questioning, I am going to try this myself and recognize myself for the first 5 minutes with a "yes" or "no" required out of each of you, and we can go down the line starting with Mr. Goldman and around and around.

So yes or no, Mr. Goldman, is the existence of so many State standards an impediment to faster consumer notification?

Mr. GOLDMAN. Yes.

Mr. HOLLEYMAN. Yes.

Mr. PRATT. Yes.

Mr. ROTENBERG. Should not be.

Mrs. BONO MACK. Is preemption necessary to speed up the consumer notification?

Mr. GOLDMAN. Yes.

Mr. HOLLEYMAN. Yes.

Mr. PRATT. Yes.

Mr. ROTENBERG. No.

Mrs. BONO MACK. Would a single Federal standard lessen the risk of over-notification and decrease the number of unnecessary notices sent every year?

Mr. GOLDMAN. Yes.

Mr. HOLLEYMAN. Yes.

Mr. PRATT. Yes.

Mr. ROTENBERG. No.

Mrs. BONO MACK. Do you think consumers can become desensitized to risk if they receive too many notifications?

Mr. GOLDMAN. Yes.

Mr. HOLLEYMAN. Yes.

Mr. PRATT. Yes.

Mr. ROTENBERG. Yes.

Mrs. BONO MACK. Do you believe there is a problem with over-notification that can adversely affect consumers even if it may be erring on the side of caution with consumers' benefits?

Mr. GOLDMAN. Yes.

Mr. HOLLEYMAN. Yes.

Mr. PRATT. Yes.

Mr. ROTENBERG. No.

Mrs. BONO MACK. Do businesses ever err on the side of notifying consumers even if they may not be required to do so, because wading through 46-plus standards is too difficult or time-consuming?

Mr. GOLDMAN. Yes.

Mr. HOLLEYMAN. Yes.

Mr. PRATT. Yes.

Mr. ROTENBERG. I don't know.

Mrs. BONO MACK. Should companies who no longer need it keep sensitive information such as credit card numbers or dates of birth in perpetuity?

Mr. GOLDMAN. Would you repeat the question? Sorry.

Mrs. BONO MACK. Should companies who no longer need it keep sensitive information such as credit card numbers or dates of birth in perpetuity?

Mr. GOLDMAN. "It depends" is not an answer, right? No.

Mr. HOLLEYMAN. I would say no.

Mr. PRATT. No.

Mr. ROTENBERG. No.

Mrs. BONO MACK. Should every data breach trigger a notice to consumers?

Mr. GOLDMAN. No.

Mr. HOLLEYMAN. No.

Mr. PRATT. No.

Mr. ROTENBERG. Yes.

Mrs. BONO MACK. Should information made available by Federal, State, or local governments in accordance with the law, and thus otherwise be publicly available, be considered personal information?

Mr. GOLDMAN. No.

Mr. HOLLEYMAN. I would not take a position on that.

Mr. PRATT. No.

Mr. ROTENBERG. Yes.

Mrs. BONO MACK. Should the FTC have the ability to modify the definition of PDI?

Mr. GOLDMAN. No.

Mr. HOLLEYMAN. I would say our answer would be yes.

Mr. PRATT. No.

Mr. ROTENBERG. Yes.

Mrs. BONO MACK. Should entities that are governed by explicit information security and breach notification requirements of other Federal laws enforced by other agencies also be subject to FTC enforcement under this draft?

Mr. GOLDMAN. No.

Mr. HOLLEYMAN. No.

Mr. PRATT. No.

Mr. ROTENBERG. Yes.

Mrs. BONO MACK. Should all entities, regardless of their size or the scope of personal data they hold, be subject to the same data security requirement rules for section 2 of this legislation?

Mr. GOLDMAN. No.

Mr. HOLLEYMAN. We have not taken a position on that.

Mr. PRATT. No.

Mr. ROTENBERG. No.

Mrs. BONO MACK. Thank you. And do you believe regulation of the collection and use of data is a data security issue?

Mr. GOLDMAN. Yes.

Mr. HOLLEYMAN. Yes.

Mr. PRATT. No.

Mr. ROTENBERG. Yes.

Mrs. BONO MACK. Do you think encrypted data that is breached should require notification?

Mr. GOLDMAN. No.

Mr. HOLLEYMAN. No.

Mr. PRATT. No.

Mr. ROTENBERG. Yes.

Mrs. BONO MACK. And lastly, should State attorney generals have the ability to enforce this law.

Mr. GOLDMAN. No.

Mr. HOLLEYMAN. Yes.

Mr. PRATT. No position.

Mr. ROTENBERG. Yes.

Mrs. BONO MACK. Is your organization a nonprofit organization?
Mr. GOLDMAN. Yes.
Mr. HOLLEYMAN. Yes.
Mr. PRATT. Yes.
Mr. ROTENBERG. Yes.
Mrs. BONO MACK. Does your organization maintain personal information of the sort that would be covered by this bill?
Mr. GOLDMAN. I don't know.
Mr. HOLLEYMAN. Yes, for our employees.
Mr. PRATT. Yes.
Mr. ROTENBERG. Yes.
Mrs. BONO MACK. Do you agree with the proposal to allow the FTC to regulate in this area?
Mr. GOLDMAN. Yes.
Mr. HOLLEYMAN. Yes.
Mr. PRATT. Yes.
Mr. ROTENBERG. Yes.
Mrs. BONO MACK. And now just the wild card, to throw it out: Do you believe political campaigns should be covered as well?
Mr. GOLDMAN. No comment.
Mr. HOLLEYMAN. Would consider it.
Mr. PRATT. No position.
Mr. ROTENBERG. Yes.
Mrs. BONO MACK. Thank you. All right. That went rather well.
Mr. Goldman, you suggest change in the time frame from 48 hours to a reasonable time frame would guard against over-notification and consumer overreaction. If notification is tied to risk of harm, how do we risk over-notification?
Mr. GOLDMAN. I think it comes down to, again, we are extremely concerned about over-notification, and specifically it depends what kind the breach is. I mean, this is one of the things I mentioned in my testimony, is that if you, for example, have an employee steal information for another employee, that is sort of a one-on-one breach; so does that trigger the whole breach mechanism that is included as part of this? So I think it sort of depends on a case-by-case basis, is what I would say.
Mrs. BONO MACK. Thank you.
And Mr. Rotenberg, you recommend that Congress define PII and not permit the FTC to further amend that definition—I mean, excuse me; Mr. Pratt, this question is for you. But is it wise to lock anything into stone when it comes to technology? Could there be advances in technology that would enable seemingly innocuous pieces of information to become the tool of fraudsters?
Mr. PRATT. As an industry that deals with a lot of that information that is sensitive and as an industry that secures that information today, I mean, we are comfortable with the structure that you have in place. We do think it encompasses the types of data that expose consumers to a degree of risk. And I think even some of the examples that Mr. Rotenberg has given, we would disagree with those, that those are necessarily new and different risks that might have to be accounted for subsequently. So we still stand by the position that we believe Congress should work out its definition and give businesses a stable marketplace in which to then compete and build the products and services.

Mrs. BONO MACK. Thank you. My time is expired. I look forward to a second round of questioning, and now recognize Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. I thank the chairman. Information brokers possess huge data profiles on a staggering number of Americans, nearly all of them—nearly all of whom do no business with these brokers. These brokers invest time and money to uncover personal details and, without knowledge or consent, they sell this information to the highest bidder. It appears that American consumers have no free market method of showing disapproval if they feel their personal information is being misused or to correct any inaccuracies in the profiles. It is in situations like these where it becomes prudent to enact laws that empower consumers, giving them the tools they need to control their personal data.

Mr. Rotenberg, do you believe, sir, that consumers should be able to access the information that brokers hold about them upon their request?

Mr. ROTENBERG. Yes, I do, Mr. Butterfield. And I do so for precisely the reason that you explained, which is that there is no one-to-one relationship between the consumer and the information broker. They are a third party, which means the consumer actually doesn't otherwise know what information they would have.

Mr. BUTTERFIELD. When a broker possesses information. Who actually owns that data?

Mr. PRATT. Well, of course the broker would claim that they do. But what they do with the data has an enormous impact on the individual. It can determine employment, it can determine whether they get an apartment, a Federal contract. A whole range of activity in the United States is today deeply impacted by the information that information brokers have about us and they make available to others.

Mr. BUTTERFIELD. Do you believe that consumers should be able to dispute inaccurate information that brokers hold on them?

Mr. ROTENBERG. Yes I do. The information brokers have become the modern-day equivalent of the credit reporting agency. And Congress figured out 40 years ago the credit reporting agencies were holding financial reports on consumers that impacted their ability to get loans and start businesses. Information brokers are playing a similar role today. Individuals should have a right to dispute what is in that record.

Mr. BUTTERFIELD. H.R. 2221, the data security bill approved by the House last Congress, that Mr. Rush and others had their fingerprints on but which the Senate failed to act, contained various requirements on how information brokers must interact with consumers seeking to access their personal information or resolve a dispute about its accuracy or misuse.

In lieu of complying with these requirements, brokers were given an alternative procedure that they could follow; namely, providing individuals with the option to completely opt out of having their personal info used for marketing purposes. Neither the special requirements on information brokers nor the alternative opt-out procedure are included in the Republican discussion draft as we can discern.

In the absence of a Federal law mandating simple opt-out procedures, brokers have generally not provided them. However, in a perverse turn the data broker, U.S. Search, Incorporated, recently tried to fill the gap by telling consumers that for $10 it would lock their record so that others could not see them or buy them. The FTC soon found this promise was entirely false. In March the Commission reached a settlement where the company agreed to refund all fees charged and avoid misrepresentations in the future.

Again, Mr. Rotenberg, do you believe that it is currently too difficult for consumers to opt out of information broker databases?

Mr. ROTENBERG. Yes, I do, Mr. Butterfield. I think this is an area where there needs to be legislative safeguards.

Mr. BUTTERFIELD. Can you discuss how difficult it is to remove one's information from a broker's database in regards to broker retailers?

Mr. ROTENBERG. Well, the broker business model relies, of course, on the collection of detailed information about consumers without their knowledge. It is not the consumers providing information. And that information gains commercial value as it is shared with more third parties. The consumer has no ability to interact to limit those transactions. So the simple answer to your question is, it is very difficult—it is very difficult I think for consumers to play any meaningful role in what information brokers do with information about them.

Mr. BUTTERFIELD. I see your point. And let me just throw it over to the chairman and yield to her.

Mrs. BONO MACK. I appreciate the gentleman yielding to me very much at a strange time.

I just want to reiterate to the panel and the subcommittee that we are also looking at privacy. And to the degree that we can separate the privacy debate from the data breach debate, it all will be helpful for us as lawmakers to understand that the two, although very similar in this case, they might be different. So I just wanted to throw that out for you all, to point out when you see it as a privacy issue beyond data breach, that would be helpful.

Mr. BUTTERFIELD. That is a very important distinction, and I thank the chairman for making that comment. My time is expired. I yield back.

Mrs. BONO MACK. Thank you very much, Mr. Butterfield. And the chair is happy to recognize Mr. Stearns for 5 minutes.

Mr. STEARNS. Thank you Madam Chair.

Mr. Goldman, the chairlady talked about this 48 hours breach. And Mr. Goldman, you had indicated that you have more preference for a reasonable, I think you indicated——

Mr. GOLDMAN. Correct.

Mr. STEARNS. Are there cases where, for example, we could move the 48 hours to, let's say 96 or 72, that you would feel more comfortable with, rather than 48 hours; or is it a fundamental idea in your mind that every company is different; one is a small company, one is a large company, the situation in which it occurs is different, so in fact to put a mandate of 48 hours as a time frame might not be applicable? So maybe you might want to explore that.

Mr. GOLDMAN. Sure. I mean, from talking to some of our members that have experienced, unfortunately, some of these breaches,

they are talking that it can take anywhere from a few days, to even 100 days or more, to get to the bottom of it. So that is why we are very leery of putting a time frame on it.

I guess H.R. 2221 included, I think, a 60-day time frame. I don't think we generally supported that bill, but I don't think we fully vetted that 60-day requirement, so I would have to get back to you on that. But I think generally we are concerned about making sure that businesses have the ability to properly react without having a time frame guide their actions.

Mr. STEARNS. Can you give me a specific example from one of your members where a 48-hour time frame would be harmful or very difficult to accomplish?

Mr. GOLDMAN. Well, I think from reading the press reports, I will speak to this. In one of the cases that recently occurred the company said, originally said, that the credit card data was compromised. And it turns out that credit card data was not compromised.

Mr. STEARNS. So it took them some time to figure it out?

Mr. GOLDMAN. It took them some time, but in the meantime they notified and told customers that their credit card data was compromised. So in the meantime you have customers canceling their credit cards, going through the inconvenience of canceling their credit card and having to get new credit cards. And it is even more of an inconvenience if you have monthly fees automatically charged to your credit card, because then you have to contact those vendors, and it just gets very complicated.

So I think from the consumer point of view, I would like to make sure before I go through that hassle that I actually have to.

Mr. STEARNS. And so when you use the language "reasonable" time period, that gives them that flexibility?

Mr. GOLDMAN. I would say so.

Mr. STEARNS. And Mr. Rotenberg, you don't agree with this. As I understand it, you think that 48 hours. But based upon what Mr. Goldman said, is there a possibility where there are situations where a company, particularly you mentioned this credit card company, that if they go out and scare all their members within this 24- or 48-hour period, these people all start canceling their credit cards, when actually when they do the investigation there was not a breach? Is that a good example or do you think that his example is——

Mr. ROTENBERG. If I may clarify, Congressman, not only do I stay by the 48-hour rule, I actually disagree with the characterization of your first witness. I know a fair amount about what happened in this Citigroup breach matter. In fact, there was credit card information disclosed; it was account holder name information and it was the account number information. Now, it was not the security code and it was not the expiration number. And the conclusion was drawn that therefore the risk was somewhat—somewhat less than they initially thought. But the risk was very real and it was important for people to be notified.

Mr. STEARNS. But would you also agree with what Mr. Goldman says, that every company is different and sometimes this breach when they are going to look at perhaps thousands and millions and tens of thousands, that it is possible that they can't do it in 48

hours, and there might be some idea, maybe not 48 and 96, there might be a reasonable time period; wouldn't you agree on that?

Mr. ROTENBERG. I appreciate the difficulty, and there is no doubt there is a real burden on companies when they have to notify customers, and they are understandably reluctant to. But there is a problem, and I don't think we can diminish the problem by——

Mr. STEARNS. OK. I want to go on. I have another question.

Mr. GOLDMAN. Just to clarify, I was not referring to Citibank, just to clarify.

Mr. STEARNS. OK. Also in the bill it talks about personal identifiable information, and we had some questions on that. Is there any—are any of you concerned about the definition of personal identifiable information? Can a company adequately understand that definition so that they can actually conclude when it comes to data minimization what they should take out?

I guess my question is, Mr. Goldman, are you concerned about the FTC and how they interpret these terms and what impact the legislation would have dealing with data minimization?

Mr. GOLDMAN. Yes, we are concerned about the ability of the FTC to expand its definition of what PII means. I think we are comfortable with the definition that is in the draft bill as is. We worry about the inclusion of Internet protocol addresses, we worry about inclusion of user names. So I think, yes, we are definitely worried about the expansion, the possibility of expansion authority.

Mr. STEARNS. Thank you, Madam Chair.

Mrs. BONO MACK. I thank the gentleman. The chair now recognizes Mr. Rush for 5 minutes.

Mr. RUSH. I want to thank you, Madam Chair.

Mr. Holleyman, you said in your testimony, and I hope that I am accurate in my paraphrasing, that security breach notifications should be required in instances where there is reasonable risk of identity theft, fraud, or unlawful conduct. You suggest that these limits are needed to help reduce excessive notifications which might lead to mass anxiety and panic among consumers. But as Mr. Rotenberg pointed out, phishing and spear fishing was the two examples of fraud and unlawful conduct likely to result in most, if not all, instances of large-scale breaches.

So should the scale of the breach be a dispositive factor in determining whether consumers also receive immediate notification?

Mr. HOLLEYMAN. Thank you, Mr. Rush. A good question. I think we believe that there should be notification triggered when there is a significant risk of a harm. We think that the important provisions in this bill, however, are the ones that encourage industry to adopt security measures, using encryption or other technologies that would render the information indecipherable or unreadable; and that that is actually, at the end of the day, the most important safeguard because that, when it is affected—if that information is obtained but the criminal can't do anything with that information, then we believe that you should not have to notify consumers, because it is that excessive notification that we believe raises consumers' concerns unnecessarily. And what the market should be doing is driving people to store data in unreadable format so that when breaches occur—and they will—the criminal can't do anything with that data.

Mr. RUSH. Do the other three witnesses agree with that?

Mr. PRATT. We strongly agree, though, that one of the—and this was true of your bill as well, Congressman, and that is the incentive to render the data unusable is probably one of the most critical provisions of the current draft of the bill that you had passed last year. It is the one that we focus on as an industry every day, it is the one that we take most seriously. Because the strong incentive is not to notify people that you have lost data, whether it is a criminal act or some other failing, but to have protected it in the first place. I mean, that is always first. Protect it in the first place. Find the best technology to do it when the data is at rest, when the data is in transmission. That is really critical.

Mr. RUSH. Mr. Pratt, you argue in your testimony for advance notice of a security breach presumably at the same time as when notice is given to the FTC. Would such a model favor your members over other similar parties who don't make the definitional cut as, quote, "data broker," end of quote?

Mr. PRATT. The reason we are requesting notice—and I am not sure we are saying that it has to occur concurrent with notification of law enforcement or the FTC—we are just simply—we have call centers, and when a letter goes out and says, call the credit bureau and order a credit report, we have to make sure that we have the right staff, we have to make sure that we have the right pipes open for the online access or the telephonic access, even the mail processing access. And we have to normalize systems. We understand what our normal pattern is.

But a very, very large data breach creates aberrant patterns which create spikes of activity. We just want to be able to serve the consumer and ensure that they get the credit report that they want, or ensure that the telephone is picked up on time, which is what they expect. So that really is the reason why we are asking for that.

Mr. RUSH. Can any of the other witnesses conceive how such a model might impede the FTC's ability to investigate and enforce under the law? Any other witnesses? All right.

OK, let me ask Mr. Rotenberg. Mr. Rotenberg, can you please elaborate further on why you believe this definition of personal information is too narrow and why you believe it should be defined as information that, quote, "identifies or could identify a particular person," end quote.

Mr. ROTENBERG. Well, I think the definition that I proposed followed with examples, which are included in the bill, is common sense. We think of personal information as information that identifies someone, or could identify them, and then the examples are good. But I also know, based on some of the recent experiences with data breaches, that an IP address poses a risk because it can be personally identifiable.

The Facebook user ID posed a risk because it was user identifiable. So the list helps people understand. But if the list is limited, I think we have a problem.

Mr. RUSH. Thank you, Madam Chair. I yield back the balance of my time.

Mrs. BONO MACK. Thank you, Mr. Rush. And the chair recognizes Mr. Olson for 5 minutes.

Mr. OLSON. I thank the chair, and I would like to welcome the witnesses. And I really appreciate your perspectives on an issue which has only become more pervasive in the future, just as Mr. Rotenberg eloquently stated in his opening statement.

My first two questions are for you, Mr. Goldman. What is the Chamber's view of the carveout for entities already covered in the Gramm-Leach-Bliley? Is this an adequate, explicit carveout?

Mr. GOLDMAN. We didn't take a position in our testimony. But generally we have supported carveouts for entities that are already covered by other laws, so there is not duplicative laws and they can figure out which agency they are better regulated under. So, yes, that is my answer.

Mr. OLSON. OK. Thank you for that answer. And as currently drafted, the legislation standard for risk is a reasonable risk of harm. When I asked our witness on a previous panel, the FTC commissioner, Ms. Ramirez, she stated that the FTC thought that reasonable risk was the right standard, because erring on the side of notification overrides some sort of desensitation of the public.

And could you elaborate on why the Chamber believes that consumers will be better off if the standard were changed to significant risk of harm?

Mr. GOLDMAN. Sure. The Chamber does support a significant risk standard because we are worried, I guess as I stated in my opening comments, about two possibilities where customers are over-notified and they just ignore it, and then when a real risk occurs they don't take any action; or they get a notice and get—and sort of reactneedlessly, and so they cancel their credit card. So both—I mean both extremes. So we prefer to have the significant risk standard.

Mr. OLSON. Thank you for that answer. And then I have got a round of questions for all four of the witnesses. And we will start off with you, Mr. Rotenberg, just to give Mr. Goldman a break here. But if you or one of your member companies suffered from a security breach, how would the proposed SAFE Data Act change their response and how would it better help consumers avoid identity theft?

Mr. ROTENBERG. Congressman, we actually don't have member companies. But I will say that many of the elements that are currently in the bill we have actually tried to follow over the years. For example, this goal of data minimization we think is a very good way to protect people online, and we have for a number of years taken steps to limit the amount of personal information that we collect. We collect information we need to provide the services that we provide, but we don't collect excessive information.

Mr. OLSON. Thank you. Mr. Pratt.

Mr. PRATT. Our members are regulated first on the data breach notification side by the 47 or 48 State statutes that are out there today. So establishing a Federal standard I think would give us an easier route to compliance. But we would be notifying consumers, just as we do today, under those State statutes. And all of our, almost all of our members are financial institutions under the Gramm-Leach-Bliley Act. And so we are already complying with a data security regime which is called the Safeguards Rule.

And so for most of our members it would not be a remarkable change. In fact, even where our members have sensitive data that isn't otherwise regulated under GLB, for example, we build enterprise-wide data security. There is no reason to segregate out some data and treat it differently from other information, so it is built enterprise-wide.

Mr. OLSON. Thank you for that answer. Mr. Holleyman.

Mr. HOLLEYMAN. I can't speak for any individual member company. But I can say that all of our companies are involved in trying to build greater security into their products in companies who provide tools to consumers and businesses to secure their environments. And certainly in supporting the concepts of this bill, we recognize that they are ones that we would be subject to. And our members with that are completely welcoming this legislation, again with some fine-tuning we would like to see. But we think it is important to act, and important to act this year.

Mr. OLSON. Thank you, sir. And finally, Mr. Goldman.

Mr. GOLDMAN. Sir, with the uniform national standard it would make it easier for our companies to comply, versus the current situation of having to comply with 46, 47 State rules. Also a lot of our companies are covered by other laws such as GLB or HIPAA.

Mr. OLSON. Well, thank you for that question. As a Navy guy, I can say to all four of you that we may not be hitting the bull's-eye but we are hitting the target.

Finally, one question for the four of you. This proposed legislation would require an entity to conduct an assessment upon discovering a breach.

Do you or one of your member companies, with all due apologies, Mr. Rotenberg, already conduct assessments? I think I know the answer. And how would this requirement and its timing impact your ability—your company's ability to members to resolve a security breach?

Mr. ROTENBERG. I will take a pass.

Mr. PRATT. I can't speak specifically, because today those assessments would be dictated by the State laws that are out there which dictate different standards. That is one of the reasons why a national standard would be helpful in terms of assessing a data breach risk.

If I could just take 1 minute to speak to this GLB exception. It is important to have this exception, because data security in this bill is a good idea, and our members are happy to live under a new data security regime for part of our businesses which might not otherwise be regulated. But if our members, small or large, are regulated by the Gramm-Leach-Bliley Act, we are only asking that we just operate in tandem, that we have the same data security provision under GLB.

That is why that exception is so important, though, because it means I don't have overlapping requirements between two different standards. And for small businesses, in particular in our membership, that is an important thing, because they don't necessarily have a general counsel on staff that is going to advise them all the time.

Mr. OLSON. Thank you for that. Mr. Holleyman.

Mr. HOLLEYMAN. Because our members oftentimes provide technologies that are used to prevent breaches, we also have a lot of experience in helping identify breaches when they occur. And we know through that, that the nature of the breach may differ, the amount of time to make the assessment may differ, and we support the provisions of the bill that are flexible, depending on the nature of the breach and the size of the enterprise.

Mr. OLSON. Thank you. And finally, Mr. Goldman.

Mrs. BONO MACK. Excuse me, we need to move on. We are a minute over.

Mr. OLSON. That was yield back time that I didn't have, but I yield back the balance of my time.

Mrs. BONO MACK. I appreciate that very much, and am happy to recognize Mr. Kinzinger for 5 minutes.

Mr. KINZINGER. Thank you, Madam Chairman. And I will say as an Air Force guy, we hit the bull's-eye on the target every time, so I think that is important to note.

Mr. OLSON. You don't want to go there, my friend.

Mr. KINZINGER. I appreciate all four of you in your assistance in helping us draft, I think, this very important piece of legislation. Some of this stuff has been touched on a little bit, but I want to make sure we are getting all the questions answered that we need.

For the three, Mr. Holleyman, Pratt, and Rotenberg, and then I guess Mr. Goldman, if you want to jump in on this too. Let me ask, in the current draft, if a company is unable to detect a breach over the course of several months due to insufficient security techniques, it does not appear that they necessarily face harsher penalties for that.

Do you believe that this legislation should include reasonable standards or methods for detecting breaches, and penalties for those companies that fail to reach those standards?

Mr. ROTENBERG. Yes, I think it is an excellent point. It would be a good change.

Mr. PRATT. We haven't actually asked our members that question, but maybe we could follow up with you and give you an answer to that. I would say in general, though, that the data security requirements that the FTC writes today are broad, they are enforced aggressively, and they would imply that you have to have sufficient security standards, not just simply to protect against, but to detect possible intrusions.

And I know even the association I run has stood up several major platforms where we have had intrusion detection systems that operate concurrently with other forms of protection of the data itself, so it is fairly common.

Mr. KINZINGER. And for those kinds of systems are they pretty foolproof?

Mr. PRATT. Well, I don't think anything is foolproof. It is a moving target. And I think that is very important for all of you—all of you all know this because of the cybersecurity issues that you probably learned about in other hearings; and that is, it is a moving target. So they are always hitting targets, but they are different targets.

Mr. KINZINGER. Right. I understand.

Mr. PRATT. But it is critical. And so when you look at these security requirements that are imposed on U.S. businesses, they are written flexibly enough to account for ongoing assessment of risk. That is one of the key components. We are comfortable with that. Because we would agree, by the way, as well that it is a business necessity that we protect the data that we have, that we use the best technologies, that we look at new risk.

Our members, for example, participate in the ISAC, which is the Information Sharing and Analysis Center that is operated by Treasury in order to see what kind of cybersecurity risks are out there, so we exchange information.

Mr. KINZINGER. Mr. Holleyman.

Mr. HOLLEYMAN. We certainly support the framework that this bill outlines. I want to get back to you on some of the specifics, particularly around newer concepts like minimization. They are important but we have to canvas our members. We do believe that this bill is important because it not only deals with the issue of notification of breaches after the fact, but it puts in place obligations related to securing data. Again, those obligations, and when businesses do that up front, that is going to minimize the need for notifications, the excessive notification. So that is an important addition to the concept of this bill.

Mr. KINZINGER. Did you want to jump in on this?

Mr. GOLDMAN. I have to go back to our members and ask, but generally companies are very concerned about reputational harm. So they are going to take, you know, for liability purposes and reputation purposes, they are going to take the best practices they can imagine.

Mr. KINZINGER. And just quickly.

Mr. PRATT. Just one point. And that is data security involves access control. Access control would almost inherently require or at least implicitly require some sort of intrusion detection system, because otherwise you are not controlling access. So I think even if it is not expressly stated, it is built into the access control concept.

Mr. KINZINGER. OK. And as we talked about, getting into the boy-who-cried-wolf issue—and if we can keep this real brief for all of you—this draft could give a company an exceedingly long period of time to notify customers in a breach of high severity.

Do you believe we should look into creating kind of tiers of risk, so if there is a high level of risk for the consumer, that notification be treated differently than that of a more moderate risk? Should we have obviously different tiers on that?

Mr. ROTENBERG. Congressman, I think that is an attractive idea, but it would actually end up adding a layer of complexity to an already serious problem. And I think it is notable when we have these extreme breach problems with Citibank, Sony, and others, very sophisticated companies, a large number of customers, here we are more than a month later and we still don't fully know the extent of the harm.

So while I appreciate the approach, I would try to go for a single simple standard. I think it is easier to manage.

Mr. KINZINGER. And if you just, very quickly, because I have one more quick question and 20 seconds.

Mr. PRATT. I would have to get back to you on that. We don't have a position on that right now.

Mr. KINZINGER. OK.

Mr. HOLLEYMAN. We believe your issue can be best addressed by using the term "significant risk" in the bill.

Mr. KINZINGER. And then, Mr. Goldman, do you believe that the legislation should more clearly define the size and scope of companies that must develop a security plan?

Mr. GOLDMAN. Yes. I mean, specifically—well, I will go back to what I said before, was that when it talks about the—you know, if you have a breach, you know, it depends on the size of the breach; and in terms of the company, yes. I mean, small businesses obviously are going to have much different capabilities to respond than a larger-size business, yes.

Mr. KINZINGER. And I yield back my negative time. Thank you, Madam Chairman.

Mrs. BONO MACK. Thank you very much, Mr. Kinzinger. And gentlemen, I would like to express the gratitude of all of the members of our subcommittee for your time today and thank you for your willingness to engage with us on this very important discussion. I think there are a lot of great ideas and willingness to come together with a great bill.

I want to reiterate again my desire for a bipartisan product, and believe that Mr. Butterfield and I can accomplish that goal. I am very hopeful for that.

I would also like to say that I was hoping for a second round of questions but time has gotten the better of us here. So I note that I will have some further questions in writing to send to all of you. And I would like to remind the members that they all have 10 business days to submit questions for the record, and would ask the witnesses to please respond promptly to any questions they receive.

Mrs. BONO MACK. So again, as the recent spate of high-profile, eye-popping data breaches point to the need for new safeguards to better protect sensitive online consumer information. It is a huge challenge and I know that we can get this done by working together.

So thank you all very much for your time today. And with that, the hearing—the subcommittee is adjourned.

[Whereupon, at 1:05 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. EDOLPHUS TOWNS

Thank you Chairman Bono-Mack and Ranking Member Butterfield for holding this legislative hearing today on "The SAFE Data Act". The issue of data theft has plagued consumers in our country for several years and currently there is no comprehensive federal law that would require companies that hold consumer's personal information to implement reasonable measures to protect that data. It is my hope that this hearing will reinforce the need to protect consumers

against fraudulent activity that target an individual's personal information. With the advent of cloud computing and the increased volume of online purchasing, data security must be at the forefront of consumer protection.

In the previous Congress members from both sides of the isle took the lead on this issue and acted in a bipartisan effort to reduce the number of data breaches while at the same time empowering consumers with new rights whenever personal information is compromised. Unfortunately time was not on our side and the Senate

was unable take on this issue of data theft before the end of the 111th Congress. Data theft still remains a very large burden for the American consumer that must be addressed by legislative action from this committee. Unfortunately the discussion draft before us today falls short of the commitment needed to ensure that the personal information of hard working Americans are kept safe.

Recent media reports pertaining to data breaches at the Sony Corporation, Epsilon Data Management and Gawker Media help to reinforce the need for congress to act once again in a bipartisan manner. I look forward to hearing from our witnesses today about how they have been dealing with this important issue. I also look forward to working with my colleagues on this committee to ensure that data security measures and protocols are enhanced in this congress to protect the American people.

Thank you Madam Chair, I yield back my time.

Responses to Questions for the Record to Com. Ramirez
June 15, 2011 Subcommittee on Commerce, Manufacturing, and Trade Hearing

1. **H.R. __ , the SAFE Data Act, requires notice to the FTC and consumers of an electronic data breach only if the person engaged in interstate commerce that owns or possesses data in electronic form containing personal information related to that commercial activity has affirmatively determined that the breach "presents a reasonable risk of identity theft, fraud, or other unlawful conduct." At the Subcommittee hearing on June 15, 2011, you indicated support for a notification standard based on "reasonable risk." In technical comments provided to the Subcommittee, FTC staff suggests that a "'reasonable risk' standard has not been applied in this context under existing law" because many state laws focus on whether there was a breach rather than the degree and type of risk to consumers. Therefore, the FTC would likely need to clarify by rulemaking what constitutes "reasonable risk."**

    a. **Please explain why you believe "reasonable risk" is the appropriate notification trigger and why it is preferable compared to other triggers - for example, one based solely on whether there was a breach (taking into account presumptions or exemptions from notification) or one based on "significant risk."**

A reasonableness standard strikes a proper balance: it requires companies to give consumers the notice they need to protect themselves when there is a risk, while reducing the likelihood that consumers will get too many notices and easing the burden that may be imposed on companies. By contrast, the other standards that are referenced may result in over-notification or under-notification. For example, requiring notification any time there has been unauthorized access to data could result in hundreds of notices to consumers when there is no risk of harm, and could lead consumers to ignore notices when they are at risk. While a trigger based solely on the occurrence of a breach could result in over-notification, one founded on a "significant risk" standard could lead to inadequate notice to consumers. This higher standard would not require notices in circumstances where a risk of harm exists but it is not deemed to be "significant" – thus depriving consumers of the opportunity to take steps to minimize the risk and avoid harm. I would expect a "significant risk" standard to result in many fewer notifications than are currently required under state law and too little protection for consumers.

    b. **Do you believe this bill should require breach notification to consumers when types of harm other than "identity theft, fraud, or other unlawful conduct" occur? If so, please explain in what ways consumers can suffer harm from the breach of their information even when they are not at risk of "identity theft, fraud, or other unlawful conduct"?**

Although the phrase "identity theft, fraud, or other unlawful conduct" encompasses a wide array

of harms, there are other harms that could result from a data breach that ought to be protected. For example, as discussed at the hearing, exposure of information regarding a consumer's medical history may not fall within the bill's harm standard, but could lead to other serious consequences, such as affecting the consumer's employment. The Commission's case against Eli Lilly and Company (*available at* http://www.ftc.gov/os/caselist/0123214/0123214.shtm), which involved exposure of consumers' use of the anti-depressant medication Prozac, highlights the need to protect against such breaches. Similarly, the disclosure of non-public communications – such as emails or the private tweets at issue in the Commission's data security case against Twitter (*available at* http://www.ftc.gov/opa/2010/06/twitter.shtm) – could also affect, among other things, consumers' employment.

2. **Under H.R. 2221, the Data Accountability and Trust Act of the 111th Congress, there was a presumption of breach notification, and to be relieved of the obligation to notify, the burden was on the company to demonstrate that there was *no risk of harm* to consumers. H.R. __, the SAFE Data Act, however, states that a company must provide notice if it *affirmatively* determines *there is a risk* to consumers. According to comments from the Center for Democracy and Technology, this distinction is "significant." CDT suggests a notice trigger based on an affirmative finding *of risk* provides an incentive to not thoroughly assess a breach for fear of finding information suggesting risk, whereas requiring a determination of *no risk* provides a greater incentive to investigate because the company can avoid notification based on the information uncovered. Do you agree or disagree that this is a significant distinction? Please explain why.**

I agree that it is preferable to require a finding of no risk rather than a finding of risk. As CDT suggests, a presumption of notification creates more incentives for companies to investigate thoroughly. By contrast, a presumption of non-notification would leave consumers in the dark in circumstances where a company has failed to conduct a reasonable investigation or where the facts are not fully known immediately but quick action by consumers (such as by placing a fraud alert) could prevent considerable harm down the road. I believe that the presumption should be to provide notice when there is a breach, unless the breached entity makes a reasonable determination that notice is not necessary based on its risk assessment. I am therefore pleased to see that the current version of the SAFE DATA Act, like H.R. 2221, requires companies to notify consumers of a breach unless they affirmatively determine that there is no reasonable risk of harm.[1]

3. **Under H.R. __, the SAFE Data Act, the term "personal information" means an individual's first name or initial and last name, or address, or phone number, in combination with anyone or more of the following data elements for that individual:**

[1] As originally introduced, the SAFE Data Act did provide that a company must provide notice if it affirmatively determines there is a risk, but it has since been amended.

a. Social Security number.

b. Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

c. Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

i. You acknowledged at the hearing that this definition was "too narrow." You mentioned the possibility of including health information in the definition. Can you be more specific regarding what you mean by health information that should be included in the definition and what other types of information should be considered "personal information?"

Failing to include health information in the bill would leave a gap in statutory protection of health information such as information about an individual's physical condition or mental health. For example, the Health Insurance Portability and Accountability Act requires data security and breach notification for health information maintained by medical providers, pharmacies, and similar entities, while the Health Information Technology for Economic and Clinical Health Act requires breach notification for information maintained in electronic personal health records. The same types of information about an individual's health that are protected by these laws, however, are not specifically protected when collected and stored by medical information websites such as WebMD, and companies may not have an obligation to give consumers notice of a breach involving that information.

The definition of personal information should also be expanded in other ways. For example, Social Security numbers alone can be used for identity theft and fraud, even when not combined with other information. In addition, information such as a user name and password that can be used to access an account – whether a financial account or another type of account – is sensitive information and should be protected, especially since passwords are frequently reused across many websites. The definition should also include such information as biometric data and geolocation data, as well as non-public emails and other confidential user-generated content.

Accordingly, I recommend that the definition of "personal information" include the following information that is sensitive in nature:

(i) Social Security number.

(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(iii) Financial account number, credit or debit card number, or any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(iv) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(v) Information that could be used to access an individual's account, such as user name and password or email address and password.

(vi) An individual's first and last name, first initial and last name, or other unique identifier in combination with:

(1) the individual's month, day, and year of birth or mother's maiden name.

(2) the individual's precise geolocation.

(3) information that relates to the individual's past, present or future physical or mental health or condition, or to the provision of health care to the individual.

(4) the individual's non-public communications or other user-created content such as emails or photographs.

ii. The scope of "personal information" subject to the data security requirements and the breach notification requirement in the draft bill is the same. Do you believe that the scope of "personal information" subject to data security requirements should be the same as that subject to a breach notification requirement? Please explain why you believe the scope of "personal information" subject to data security requirements should be the same as that subject to a notification requirement, or why you believe the scope should be broader, if that is the case.

I believe the scope should be the same for both data security and breach notification, provided "personal information" is defined in a way that is sufficiently protective of consumers. The proposed definition of "personal information" discussed above, includes the most sensitive types of consumer information. Entities should be required to give consumers notice of breaches involving these sensitive types of consumer information so that affected consumers will know that their information has been exposed and can take appropriate measures to mitigate harm. Breach notification can also serve a signaling purpose: if one company experiences a number of breaches, consumers may conclude that the company does not take the security of customer

information seriously and take their business elsewhere. These same categories of personal information should also be incorporated into the substantive data security requirements so that the Commission can enforce the law to ensure that companies take appropriate measures to protect this sensitive information even if there has not been a breach.

4. **Under H.R. 2221, the Data Accountability and Trust Act of the 111th Congress, there were additional information security requirements in Section 2 that applied only to information brokers. For example, information brokers had to submit their security policies for FTC review, the FTC could conduct audits of the security practices of information brokers that experienced breaches, and information brokers had to provide certain access and correction rights to consumers. Under H.R. __, the SAFE Data Act, no additional requirements exist. Does the FTC have authority under the SAFE Data Act to - through regulation - create additional information security requirements for information brokers? For example, could FTC require information brokers to submit their security policies for FTC review? Could FTC conduct audits of the security practices of information brokers that experienced breaches? Could the FTC require information brokers to provide certain access and correction rights to consumers?**

I do not read the bill as authorizing FTC rulemaking to create additional requirements for information brokers such as requiring them to submit security policies for FTC review, obtain audits of their security practices if they experience breaches, or provide certain access and correction rights to consumers. If Congress intends to give the FTC authority to promulgate rules relating to information brokers' practices, the bill should grant the FTC specific authority to do so.